日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年　７月１６日

出 願 番 号
Application Number: 平成１０年特許願第２０１４９７号

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年　５月２１日

特 許 庁 長 官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３０３２４８２

【書類名】　特許願

【整理番号】　9800693304

【提出日】　平成10年 7月16日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/14

【発明の名称】　情報処理装置および情報処理方法

【請求項の数】　10

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　日下部　進

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　高田　昌幸

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐々木　将央

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および情報処理方法

【特許請求の範囲】

【請求項１】　データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と

を備えるデータ記憶装置に対して、前記管理情報を提供するための処理を行う情報処理装置であって、

前記管理情報を作成する作成手段と、

前記管理情報を暗号化する暗号化手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記管理情報が改竄されたか否かをチェックするためのチェックコードを演算する演算手段をさらに備え、

前記暗号化手段は、前記管理情報とともに、前記チェックコードも暗号化することを特徴とする請求項１に記載の情報処理装置。

【請求項３】　暗号化された前記管理情報を、所定の伝送媒体を介して、前記データ記憶装置に送信する送信手段をさらに備える

ことを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記管理手段が、前記データ記憶手段の記憶領域を階層構造にして管理する場合において、

前記暗号化手段は、親の階層の前記管理情報に含まれる前記キーを用いて、その子の階層の前記管理情報を暗号化する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項５】　データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と

を備えるデータ記憶装置に対して、前記管理情報を提供するための処理を行う

情報処理方法であって、

前記管理情報を作成する作成ステップと、

前記管理情報を暗号化する暗号化ステップと

を備えることを特徴とする情報処理方法。

【請求項６】　データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と

を備える情報処理装置であって、

暗号化された前記管理情報を受信する受信手段と、

暗号化された前記管理情報を復号する復号手段と、

前記管理情報を、前記管理情報記憶手段に記憶させる記憶制御手段と

を備えることを特徴とする情報処理装置。

【請求項７】　前記管理情報が改竄されたか否かをチェックするチェック手段をさらに備える

ことを特徴とする請求項６に記載の情報処理装置。

【請求項８】　前記受信手段は、暗号化された前記管理情報とともに、その管理情報が改竄されたか否かをチェックするためのチェックコードも受信し、

前記チェック手段は、前記チェックコードに基づいて、前記管理情報が改竄されたか否かのチェックを行う

ことを特徴とする請求項７に記載の情報処理装置。

【請求項９】　前記管理手段が、前記データ記憶手段の記憶領域を階層構造にして管理しており、

前記管理情報が、その親の階層の管理情報に含まれる前記キーを用いて暗号化されている場合において、

前記復号手段は、暗号化された前記管理情報を、前記管理情報記憶手段に記憶されている、その親の階層の管理情報に含まれる前記キーを用いて復号する

ことを特徴とする請求項６に記載の情報処理装置。

【請求項１０】　データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と

を備える情報処理装置の情報処理方法であって、

暗号化された前記管理情報を受信する受信ステップと、

暗号化された前記管理情報を復号する復号ステップと、

前記管理情報を、前記管理情報記憶手段に記憶させる記憶制御ステップと

を備えることを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および情報処理方法に関し、例えば、ＩＣ（Integrated Circuit）カードを回収しなくても、その内蔵するメモリを管理するための管理情報を、安全に、追加したり変更したりすることができるようにする情報処理装置および情報処理方法に関する。

【０００２】

【従来の技術】

例えば、電子マネーシステムやセキュリティシステムなどでの利用が期待されているＩＣカード（スマートカード）が開発されている。

【０００３】

ＩＣカードは、各種処理を行うＣＰＵや、処理に必要なデータなどを記憶するメモリを内蔵しており、所定のリーダ／ライタ（Ｒ／Ｗ）に電気的に接触させた状態で、または電磁波を利用して非接触で、データの送受信が行われる。なお、Ｒ／Ｗとの間で、電磁波を利用して非接触でデータの送受信を行うＩＣカードには、一般に、その電磁波により、必要な電力が供給される。

【０００４】

【発明が解決しようとする課題】

ＩＣカードを、例えば、電子マネーシステムやセキュリティシステムなどで利

用する場合においては、データの隠匿性や、ＩＣカードの偽造を防止すること等のセキュリティが重要であり、一般には、システムの管理者（運用者）によって与えられるキーによって、ＩＣカードに対するアクセスが可能となる。即ち、キーを有しない者のＩＣカードへのアクセスは制限される。

【０００５】

また、例えば、接触式のＩＣカードの標準を規定するＩＳＯ（International Organization for Standardizaion）７８１６などでも、セキュリティについて規定されており、これによれば、ディレクトリまたはフォルダに相当するＤＦ（Dedicated File）に鍵をかけることで、そのＤＦの階層に属するＤＦや、ファイルに相当するＥＦ（Elementary File）へのアクセスが制限される。

【０００６】

ところで、ＩＣカードに対して、新サービスを提供するためのデータを保持するファイルを新たに追加したり、また、データのアクセスに必要なキーを変更したりするための、いわゆる発券作業は、一般に、ユーザに発行し、市場に出回っているＩＣカードを、そのＩＣカードの管理者や製造メーカなどが回収し、セキュリティ管理の整備された施設等で行われる。

【０００７】

即ち、一般に、ＩＣカードは、例えば、図３１に示すように、ＩＣカードの発行者が、１次発行作業を行い、ファンクションのないＩＣカード（データの読み書きのできない状態のＩＣカード）を、発券作業を行う発券業者に発行する。発券業者は、そのＩＣカードによってサービスを提供しようとする管理者＃１がＩＣカードを利用することができるように発券作業（２次発行作業）を行う。即ち、発券業者は、ＩＣカードの中に、管理者＃１が利用する記憶領域（管理者＃１の領域）を確保し、さらに、管理者＃１が、その記憶領域にアクセスするのに必要なキーその他の情報を書き込む。ここで、発券作業は、例えば、発券業者の施設などの、セキュリティ管理の整備された場所（以下、適宜、安全な場所という）で行われる。また、図３１において、発券業者および管理者＃１は、同一人である場合が多い。

【０００８】

発券作業の行われたＩＣカードは、市場に出荷され、ユーザに配布等される。そして、管理者＃１がサービスを提供するのに利用される。即ち、これにより、ユーザは、ＩＣカードを、例えば、電子的な定期券や財布として利用することができる。

【０００９】

以上のようにして市場に出回ったＩＣカードが、例えば、マルチファンクションのものであり、管理者＃１以外の管理者＃２が、そのマルチファンクションのＩＣカードによってサービスの提供を行おうとする場合には、発券業者は、図３２に示すように、市場に出回っているＩＣカードを、一旦回収する。そして、発券業者は、管理者＃２がＩＣカードを利用することができるように発券作業を行う。即ち、ＩＣカードの中に、管理者＃２が利用する記憶領域（管理者＃２の領域）を確保し、さらに、管理者＃２が、その記憶領域にアクセスするのに必要なキーその他の情報を書き込む。その後、発券作業の行われたＩＣカードは、再び、市場に出荷される。

【００１０】

発券作業によってＩＣカードに書き込まれる、例えば、キーなどは、ＩＣカードのセキュリティ上重要な情報であり、このような情報を、市場などの、盗聴や改竄等の不正行為が行われる蓋然性の高い、セキュリティ管理のなされていない場所（以下、適宜、安全でない場所という）に流通させることは好ましくない。このため、発券作業は、上述のように、ＩＣカードを、市場から回収し、安全な場所で行われる。

【００１１】

従って、発券作業を行うごとに、ＩＣカードを回収しなければならず、面倒であった。

【００１２】

本発明は、このような状況に鑑みてなされたものであり、記憶領域にアクセスするのに必要なキーその他の情報を、セキュリティ上安全でない場所においても、安全に書き込むことができるようにするものである。

【００１３】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化する暗号化手段を備えることを特徴とする。

【００１４】

請求項５に記載の情報処理方法は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化する暗号化ステップを備えることを特徴とする。

【００１５】

請求項６に記載の情報処理装置は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号する復号手段を備えることを特徴とする。

【００１６】

請求項１０に記載の情報処理方法は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号する復号ステップを備えることを特徴とする。

【００１７】

請求項１に記載の情報処理装置においては、暗号化手段が、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化するようになされている。

【００１８】

請求項５に記載の情報処理方法においては、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化するようになされている。

【００１９】

請求項６に記載の情報処理装置においては、復号手段が、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号するようになされている。

【００２０】

請求項１０に記載の情報処理方法においては、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号するようになされている。

【００２１】

【発明の実施の形態】

以下に、本発明の実施の形態を説明するが、その前に、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し、一例）を付加して、本発明の特徴を記述すると、次のようになる。

【００２２】

即ち、請求項１に記載の情報処理装置は、データを記憶するデータ記憶手段（例えば、図３に示すＥＥＰＲＯＭ６６など）と、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段（例えば、図３に示すＥＥＰＲＯＭ６６など）と、管理情報に基づいて、データ記憶手段を管理する管理手段（例えば、図３に示すシーケンサ９１など）とを備えるデータ記憶装置に対して、管理情報を提供するための処理を行う情報処理装置であって、管理情報を作成する作成手段（例えば、図２８に示すプログラムの処理ステップＳ２１など）と、管理情報を暗号化する暗号化手段（例えば、図２８に示すプログラムの処理ステップＳ２３など）とを備えることを特徴とする。

【００２３】

請求項２に記載の情報処理装置は、管理情報が改竄されたか否かをチェックするためのチェックコードを演算する演算手段（例えば、図２８に示すプログラムの処理ステップＳ２２など）をさらに備え、暗号化手段が、管理情報とともに、チェックコードも暗号化することを特徴とする。

【００２４】

請求項３に記載の情報処理装置は、暗号化された管理情報を、所定の伝送媒体を介して、データ記憶装置に送信する送信手段（例えば、図２８に示すプログラ

ムの処理ステップＳ２４など）をさらに備えることを特徴とする。

【００２５】

請求項６に記載の情報処理装置は、データを記憶するデータ記憶手段（例えば、図３に示すＥＥＰＲＯＭ６６など）と、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段（例えば、図３に示すＥＥＰＲＯＭ６６など）と、管理情報に基づいて、データ記憶手段を管理する管理手段（例えば、図３に示すシーケンサ９１など）とを備える情報処理装置であって、暗号化された管理情報を受信する受信手段（例えば、図３に示すインターフェイス部６１など）と、暗号化された管理情報を復号する復号手段（例えば、図３０に示すプログラムの処理ステップＳ３２など）と、管理情報を、管理情報記憶手段に記憶させる記憶制御手段（例えば、図７に示すプログラムの処理ステップＳ４や、図８に示すプログラムの処理ステップＳ１４など）とを備えることを特徴とする。

【００２６】

請求項７に記載の情報処理装置は、管理情報が改竄されたか否かをチェックするチェック手段（例えば、図３０に示すプログラムの処理ステップＳ３３など）をさらに備えることを特徴とする。

【００２７】

なお、勿論この記載は、各手段を上記したものに限定することを意味するものではない。

【００２８】

図１は、本発明を適用したＩＣカードを用いた非接触カードシステム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の一実施の形態の構成例を示している。

【００２９】

この非接触カードシステムは、Ｒ／Ｗ１，ＩＣカード２、およびコントローラ３で構成され、Ｒ／Ｗ１とＩＣカード２との間では、電磁波を利用して非接触で、データの送受信が行われるようになされている。

【００３０】

即ち、Ｒ／Ｗ１が、所定のコマンドをＩＣカード２に送信し、ＩＣカード２は、そのコマンドを受信し、そのコマンドに対応する処理を行う。そして、ＩＣカード２は、その処理結果に対応する応答データをＲ／Ｗ１に送信する。

【００３１】

Ｒ／Ｗ１は、所定のインタフェース（例えば、ＲＳ－４８５Ａの規格などに準拠したもの）を介してコントローラ３に接続されており、コントローラ３は、Ｒ／Ｗ１に対して所定の制御信号を供給することで、所定の処理を行わせる。

【００３２】

図２は、図１のＲ／Ｗ１の構成例を示している。

【００３３】

ＩＣ２１においては、データの処理を行うＤＰＵ（Data Processing Unit）３１、ＩＣカード２に送信するデータおよびＩＣカード２から受信したデータの処理を行うＳＰＵ（Signal Processing Unit）３２、コントローラ３との通信を行うＳＣＣ（Serial Communication Controller）３３、およびデータの処理に必要な情報を予め記憶しているＲＯＭ部４１と処理途中のデータを一時的に記憶するＲＡＭ部４２とで構成されるメモリ部３４が、バスを介して接続されている。

【００３４】

また、このバスには、所定のデータを記憶するフラッシュメモリ２２も接続されている。

【００３５】

ＤＰＵ３１は、ＩＣカード２に送信するコマンドをＳＰＵ３２に出力するとともに、ＩＣカード２から受信した応答データをＳＰＵ３２から受け取るようになされている。

【００３６】

ＳＰＵ３２は、ＩＣカード２に送信するコマンドに対して所定の処理（例えば、ＢＰＳＫ（BiPhase Shift Keying）変調（ワンチェスタコードへのコーディング）など）を行った後、変調回路２３に出力するとともに、ＩＣカード２により送信されてきた応答データを復調回路２５から受け取り、そのデータに対して所

定の処理を施すようになされている。

【００３７】

変調回路２３は、発振器（ＯＳＣ）２６より供給される所定の周波数（例えば１３．５６ＭＨｚ）の搬送波を、ＳＰＵ３２より供給されるデータで、ＡＳＫ（Amplitude Shift Keying）変調し、生成された変調波をアンテナ２７を介して、電磁波としてＩＣカード２に出力するようになされている。なお、このとき、変調回路２３は、変調度を１未満にして、ＡＳＫ変調を行うようになされており、これにより、データがローレベルのときにおいても、変調波の最大振幅がゼロにならないようになされている。

【００３８】

復調回路２５は、アンテナ２７を介して受信した変調波（ＡＳＫ変調波）を復調し、復調されたデータをＳＰＵ３２に出力するようになされている。

【００３９】

図３は、図１のＩＣカード２の構成例を示している。

【００４０】

このＩＣカード２においては、ＩＣ５１が、アンテナ５３を介して、Ｒ／Ｗ１により送信された変調波を受信するようになされている。なお、コンデンサ５２は、アンテナ５３とともにＬＣ回路を構成し、所定の周波数（キャリア周波数）の電磁波に同調（共振）するようになされている。

【００４１】

ＩＣ５１において、ＲＦインタフェース部６１は、ＡＳＫ復調部８１で、アンテナ５３を介して受信した変調波（ＡＳＫ変調波）を検波して復調し、復調後のデータを、ＢＰＳＫ復調回路６２およびＰＬＬ（Phase Locked Loop）部６３に出力するとともに、電圧レギュレータ８２で、ＡＳＫ復調部８１が検波した信号を安定化し、各回路に直流電源として供給するようになされている。

【００４２】

また、ＲＦインタフェース部６１は、発振回路８３でデータのクロック周波数と同一の周波数の信号を発振し、その信号をＰＬＬ部６３に出力するようになされている。

【００４３】

さらに、ＲＦインタフェース部６１では、ＡＳＫ変調部８１において、演算部６４より、ＢＰＳＫ変調回路６８を介して供給されるデータに対応して、ＩＣカード２の電源としてのアンテナ５３の負荷を変動させる（例えば、データに対応して所定のスイッチング素子をオン／オフさせ、スイッチング素子がオン状態であるときだけ所定の負荷をアンテナ５３に並列に接続させる）ことにより、アンテナ５３を介して受信している変調波をＡＳＫ変調し（ＩＣカード２からデータを送信するときは（ＩＣカード２にデータを送信させるときは）、Ｒ／Ｗ１は、その出力する変調波の最大振幅を一定にしており、この変調波が、アンテナ５３の負荷の変動により、ＡＳＫ変調される）、その変調成分を、アンテナ５３を介してＲ／Ｗ１に送信する（Ｒ／Ｗ１のアンテナ２７の端子電圧を変動させる）ようになされている。

【００４４】

ＰＬＬ部６３は、ＡＳＫ復調部８１より供給されるデータから、そのデータに同期したクロック信号を生成し、そのクロック信号をＢＰＳＫ復調回路６２およびＢＰＳＫ変調回路６８に出力するようになされている。

【００４５】

ＢＰＳＫ復調回路６２は、ＡＳＫ復調部８１で復調されたデータが、ＢＰＳＫ変調されている場合、ＰＬＬ部６３より供給されたクロック信号に従って、そのデータの復調（ワンチェスタコードのデコード）を行い、復調したデータを演算部６４に出力するようになされている。

【００４６】

演算部６４は、ＢＰＳＫ復調回路６２より供給されたデータが暗号化されている場合、そのデータを暗号／復号部９２で復号化した後、そのデータを、シーケンサ９１で処理するようになされている。なお、データが暗号化されていない場合、ＢＰＳＫ復調回路６２より供給されたデータは、暗号／復号部９２を介さず、シーケンサ９１に、直接供給される。

【００４７】

シーケンサ９１は、そこに供給されるコマンドとしてのデータに対応する処理

を行うようになされている。即ち、例えば、シーケンサ９１は、ＥＥＰＲＯＭ６６に対するデータの書き込みや読み出し、その他データに対する必要な演算処理などを行う。さらに、シーケンサ９１は、認証を行うことによるＥＥＰＲＯＭ６６へのアクセス制御や、ＥＥＰＲＯＭ６６の管理などをも行うようになされている。

【００４８】

演算部６４のパリティ演算部９３は、ＥＥＰＲＯＭ６６に記憶されるデータや、ＥＥＰＲＯＭ６６に記憶されているデータから、パリティとして、例えば、リードソロモン符号を算出するようになされている。

【００４９】

さらに、演算部６４は、シーケンサ９１で所定の処理を行った後、その処理に対応する応答データ（Ｒ／Ｗ１に送信するデータ）をＢＰＳＫ変調回路６８に出力するようになされている。

【００５０】

ＢＰＳＫ変調回路６８は、演算部６４より供給されたデータをＢＰＳＫ変調し、変調後のデータをＲＦインタフェース部６１のＡＳＫ変調部８４に出力するようになされている。

【００５１】

ＲＯＭ（Read Only Memory）６５は、シーケンサ９１が処理を行うためのプログラムその他の必要なデータを記憶している。ＲＡＭ６７は、シーケンサ９１が処理を行うとき、その処理の途中のデータなどを、一時的に記憶するようになされている。

【００５２】

ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）６６は、不揮発性のメモリであり、ＩＣカード２がＲ／Ｗ１との通信を終了し、電力供給が停止した後も、データを記憶し続けるようになされている。

【００５３】

次に、Ｒ／Ｗ１とＩＣカード２との間のデータの送受信処理について説明する。

【００５４】

Ｒ／Ｗ１（図２）は、アンテナ２７から所定の電磁波を放射して、アンテナ２７の負荷状態を監視し、ＩＣカード２が接近することによる負荷状態の変化が検出されるまで待機する。なお、Ｒ／Ｗ１には、所定の短いパターンのデータでＡＳＫ変調した電磁波を放射して、ＩＣカード２への呼びかけを、ＩＣカード２からの応答が一定時間内に得られるまで繰り返す処理（ポーリング）を行わせるようにしてもよい。

【００５５】

Ｒ／Ｗ１において、ＩＣカード２の接近が検出されると、Ｒ／Ｗ１のＳＰＵ３２は、所定の周波数（例えば、データのクロック周波数の２倍の周波数）の矩形波を搬送波として、ＩＣカード２に送信するデータ（ＩＣカード２に実行させる処理に対応するコマンドや、ＩＣカード２に書き込むデータなど）で、ＢＰＳＫ変調を行い、生成した変調波（ＢＰＳＫ変調信号）（ワンチェスタコード）を変調回路２３に出力する。

【００５６】

なお、ＢＰＳＫ変調時においては、差動変換を利用して、変調波の位相の変化に、データを対応させることができ、このようにした場合、ＢＰＳＫ変調信号が反転しても、元のデータに復調されるので、復調するとき変調波の極性を配慮する必要が無くなる。

【００５７】

変調回路２３は、入力されたＢＰＳＫ変調信号で、所定の搬送波を１未満（例えば０．１）の変調度（＝データ信号の最大振幅／搬送波の最大振幅）でＡＳＫ変調し、生成された変調波（ＡＳＫ変調波）を、アンテナ２７を介してＩＣカード２に送信する。

【００５８】

なお、送信を行わないとき、変調回路２３は、ディジタル信号の２つのレベル（ハイレベルとローレベル）のうちの、例えばハイレベルで変調波を生成するようになされている。

【００５９】

ＩＣカード２（図３）では、アンテナ５３およびコンデンサ５２で構成されるＬＣ回路において、Ｒ／Ｗ１のアンテナ２７が放射した電磁波の一部が電気信号に変換され、その電気信号（変調波）が、ＩＣ５１のＲＦインタフェース６１に出力される。そして、ＲＦインタフェース６１のＡＳＫ復調部８１は、その変調波を整流平滑化することで、包絡線検波を行い、これにより生成される信号を電圧レギュレータ８２に供給するとともに、その信号の直流成分を抑制してデータ信号を抽出し、そのデータ信号をＢＰＳＫ復調回路６２およびＰＬＬ部６３に出力する。

【００６０】

なお、このとき、アンテナ５３の端子電圧V_0は、例えば次のようになる。

$$V_0=V_{10}(1+k\times Vs(t))\cos(\omega t)$$

但し、$V_{10}\cos(\omega t)$は、搬送波を、ｋは変調度を、Ｖｓ（ｔ）はＳＰＵ３２が出力するデータを、それぞれ表す。

【００６１】

また、ＡＳＫ復調部８１による整流後の電圧V_1におけるローレベルの値V_{LR}は、例えば次のようになる。

$$V_{LR}=V_{10}(1+k\times(-1))-Vf$$

【００６２】

ここで、Ｖｆは、ＡＳＫ復調部８１において、整流平滑化を行うための整流回路を構成するダイオード（図示せず）における電圧降下を示しており、一般に０．７ボルト程度である。

【００６３】

電圧レギュレータ８２は、ＡＳＫ復調部８１により整流平滑化された信号を受信すると、その信号を安定化し、直流電源として、演算部６４を始めとする各回路に供給する。なお、ここでは、上述したように、変調波の変調度ｋは１未満であるので、整流後の電圧変動（ハイレベルとローレベルの差）が小さい。従って、電圧レギュレータ８２において、直流電源を容易に生成することができる。

【００６４】

ここで、例えば、変調度ｋが５％の変調波を、V_{10}が３ボルト以上になるように受信した場合、整流後のローレベル電圧V_{LR}は、２．１５（＝３×（１－０．０５）－０．７）ボルト以上となり、電圧レギュレータ８２は、電源として充分な電圧を各回路に供給することができる。さらに、この場合、整流後の電圧V_1の交流成分（データ成分）の振幅２×ｋ×V_{10}（Peak-to-Peak値）は、０．３（＝２×０．０５×３）ボルト以上になり、ＡＳＫ復調部８１は、十分高いＳ／Ｎ比でデータの復調を行うことができる。

【００６５】

このように、変調度ｋが１未満のＡＳＫ変調波を利用することにより、エラーレートの低い（Ｓ／Ｎ比の高い状態で）通信を行うとともに、電源として充分な直流電圧がＩＣカード２に供給される。

【００６６】

ＢＰＳＫ復調回路６２は、ＡＳＫ復調部８１からデータ信号（ＢＰＳＫ変調信号）を受信すると、そのデータ信号を、ＰＬＬ部６３より供給されるクロック信号に従って復調し、復調したデータを演算部６４に出力する。

【００６７】

演算部６４は、ＢＰＳＫ復調回路６２より供給されたデータが暗号化されている場合は、暗号／復号部９２で復号化した後、そのデータ（コマンド）をシーケンサ９１に供給して処理する。なお、この期間、即ち、ＩＣカード２にデータを送信後、それに対する返答を受信するまでの間、Ｒ／Ｗ１は、値が１のデータを送信したまま待機している。従って、この期間においては、ＩＣカード２は、最大振幅が一定である変調波を受信している。

【００６８】

シーケンサ９１は、処理が終了すると、その処理結果などについてのデータ（Ｒ／Ｗ１に送信するデータ）を、ＢＰＳＫ変調回路６８に出力する。ＢＰＳＫ変調回路６８は、Ｒ／Ｗ１のＳＰＵ３２と同様に、そのデータをＢＰＳＫ変調（ワンチェスタコードにコーディング）した後、ＲＦインタフェース部６１のＡＳＫ変調部８４に出力する。

【００６９】

そして、ＡＳＫ変調部８４は、アンテナ５３の両端に接続される負荷を、スイッチング素子などを利用し、ＢＰＳＫ変調回路６８からのデータに応じて変動させることにより、受信している変調波（ＩＣカード２によるデータの送信時においては、上述したように、Ｒ／Ｗ１が出力する変調波の最大振幅は一定になっている）を、送信するデータに応じてＡＳＫ変調し、これによりＲ／Ｗ１のアンテナ２７の端子電圧を変動させて、そのデータをＲ／Ｗ１に送信する。

【００７０】

一方、Ｒ／Ｗ１の変調回路２３は、ＩＣカード２からのデータの受信時においては、値が１（ハイレベル）のデータの送信を継続している。そして、復調回路２５において、ＩＣカード２のアンテナ５３と電磁気的に結合しているアンテナ２７の端子電圧の微小な変動（例えば、数十マイクロボルト）から、ＩＣカード２により送信されてきたデータが検出される。

【００７１】

さらに、復調回路２５では、検出した信号（ＡＳＫ変調波）が高利得の増幅器（図示せず）で増幅されて復調され、その結果得られるディジタルデータがＳＰＵ３２に出力される。ＳＰＵ３２は、そのデータ（ＢＰＳＫ変調信号）を復調し、ＤＰＵ３１に出力する。ＤＰＵ３１は、ＳＰＵ３２からのデータを処理し、その処理結果に応じて、通信を終了するか否かを判断する。そして、再度、通信を行うと判断した場合、上述した場合と同様にして、Ｒ／Ｗ１とＩＣカード２との間で通信が行われる。一方、通信を終了すると判断した場合、Ｒ／Ｗ１は、ＩＣカード２との通信処理を終了する。

【００７２】

以上のように、Ｒ／Ｗ１は、変調度ｋが１未満であるＡＳＫ変調を利用して、ＩＣカード２にデータを送信し、ＩＣカード２は、そのデータを受け取り、そのデータに対応する処理を行って、その処理の結果に対応するデータを、Ｒ／Ｗ１に返送する。

【００７３】

次に、図４は、図３のＥＥＰＲＯＭ６６の論理フォーマットを示している。

【００７４】

ＥＥＰＲＯＭ６６は、ブロックを単位として構成され、図４の実施の形態では、１ブロックは、例えば、１６バイトで構成されている。

【００７５】

さらに、図４の実施の形態では、最も上のブロックの論理アドレスを＃００００ｈ（ｈは、１６進数を表す）として、昇順に、論理アドレスが付されている。なお、図４では、論理アドレスとして、＃００００ｈ乃至＃ＦＦＦＦｈが付されており、従って、６５５３６（＝2^{16}）個のブロックが構成されている。

【００７６】

ブロックは、ユーザブロックまたはシステムブロックとして使用されるようになされている。ＥＥＰＲＯＭ６６のブロックは、論理アドレスの昇順に、ユーザブロックに割り当てられていき、また、論理アドレスの降順に、システムブロックに割り当てられていくようになされている。即ち、図４において、ユーザブロックは下方向に、システムブロックは上方向に、それぞれ増えていき、空きブロックがなくなった時点で、ユーザブロックおよびシステムブロックをつくることはできなくなる。従って、ユーザブロックとシステムブロックとの境界は固定ではなく、また、ユーザブロックの数、またはシステムブロックの数それぞれには、特に制限がない（但し、図４の実施の形態では、ユーザブロックとシステムブロックとの合計は、６５５３６個以下に制限される）。

【００７７】

システムブロックには、製造ＩＤ（Identification）ブロック、発行ＩＤブロック、システム定義ブロック、エリア定義ブロック、サービス定義ブロックの５種類がある。なお、図４の実施の形態では、エリア定義ブロックまたはサービス定義ブロックとなっているブロックを、エリア／サービス定義ブロックと示してある。

【００７８】

システムブロックのうち、製造ＩＤブロック、発行ＩＤブロック、システム定義ブロックの３つは、基本的に、ＩＣカード２の発行時には、既に配置されているもので、論理アドレス＃ＦＦＦＦｈ，＃ＦＦＦＥｈ，＃ＦＦＦＤｈにそれぞれ

配置される。そして、エリア／サービス定義ブロックは、論理アドレス＃ＦＦＦＣｈより上に、作成順に配置されていく。

【００７９】

製造ＩＤブロックには、ＩＣカード２の製造に関する情報が配置される。即ち、製造ＩＤブロックには、例えば、ユニークな製造ＩＤや、製造年月日、製造者のコードなどが配置される。

【００８０】

発行ＩＤブロックには、ＩＣカード２の発行に関する情報が配置される。即ち、発行ＩＤブロックには、例えば、ＩＣカード２が発行された日付や、ＩＣカードを発行した順番を表すコードなどが配置される。

【００８１】

システム定義ブロックには、例えば、ＥＥＰＲＯＭ６６が有するシステムブロックまたはユーザブロックの数や、システムキーなどが配置される。なお、システムキーは、ＩＣカード２と、Ｒ／Ｗ１およびコントローラ３との間で、相互認証を行うときに用いられる。

【００８２】

エリア定義ブロックは、例えば、ＥＥＰＲＯＭ６６の記憶領域（エリア）が、管理者に割り当てられることにより作成され、そこには、管理者が、自身に割り当てられた記憶領域を管理するための情報などが配置される。即ち、エリア定義ブロックには、例えば、後述するコード範囲、空き容量、およびエリアキーなどが配置される。

【００８３】

サービス定義ブロックには、後述するサービス領域を管理するための情報（サービス領域の容量やサービスキーなど）などが配置される。

【００８４】

次に、シーケンサ９１では、ＥＥＰＲＯＭ６６の記憶領域が階層化されて管理されるようになされている。

【００８５】

即ち、図５は、ＥＥＰＲＯＭ６６のディレクトリ構造を示している。

【００８６】

ＥＥＰＲＯＭ６６の記憶領域は、エリア定義領域を階層とする階層構造をなしており、エリア定義領域は、エリア定義領域およびサービス定義領域を有することができるようになされている。

【００８７】

エリア定義領域は、管理者に割り当てられ、そこには、管理者が、エリア定義領域やサービス定義領域を識別するための名前として使用可能な識別コードの範囲を表すコード範囲、使用可能な空きブロック数を表す空き容量、認証に用いる、後述するアクセスキーを生成するためのエリアキーなどが配置される。ここで、１のエリア定義領域は、図４で説明した１のエリア定義ブロックに対応する。

【００８８】

図５の実施の形態では、管理者Ａに割り当てられたエリア定義領域が最上位階層を構成しており、これを親の階層として、管理者Ｂ１およびＢ２のエリア定義領域が作成されている。さらに、管理者Ｂ１のエリア定義領域を、親の階層として、管理者Ｃのエリア定義領域が作成されている。

【００８９】

サービス定義領域は、管理者が提供するサービスに割り当てられ、そこには、そのサービスの提供に必要なデータを記憶するサービス領域の容量や、アクセスキーを生成するためのサービスキーなどが配置される。ここで、１のサービス定義領域は、図４で説明した１のサービス定義ブロックに対応する。

【００９０】

サービス領域は、サービスの提供に必要なデータが記憶される記憶領域で、図４のユーザブロックに対応する。即ち、サービス領域は、０以上のユーザブロックで構成され、サービス領域を構成するユーザブロック数が、そのサービス領域を管理するサービス定義領域の容量として配置される。

【００９１】

また、エリア定義領域およびサービス定義領域には、それらを識別するための識別コードも配置される。ここで、エリア定義領域またはサービス定義領域を識別するための識別コードそれぞれを、以下、適宜、エリアコードまたはサービス

コードという。なお、サービスコードは、あるサービス領域を管理するサービス定義領域を識別するものであるから、そのサービス領域を識別する識別コード（サービス領域識別コード）であるということもできる。

【００９２】

図５の実施の形態では、管理者Ａに、最上位階層のエリア定義領域が割り当てられている。そして、使用可能な識別コードの範囲（コード範囲）として、０００ｈ乃至ＦＦＦＦｈが、エリアキーとして、0123456789abcdefが、それぞれ定義されている。ここで、エリア定義領域におけるコード範囲内の識別コードであれば、いずれの識別コードも、そのエリア定義領域のエリアコードとして使用可能であるが、本実施の形態では、例えば、エリア定義領域のコード範囲の最小値が、そのエリアコードとして使用されるようになされている。従って、コード範囲が、０００００ｈ乃至ＦＦＦＦｈとなっているエリア定義領域、即ち、管理者Ａに割り当てられているエリア定義領域のエリアコードは、０００００ｈとなっている。ここで、エリアコード＃ｘｘｘｘｈのエリア定義領域を、以下、適宜、エリア定義領域＃ｘｘｘｘｈと記載する。

【００９３】

管理者Ａのエリア定義領域＃０００００ｈの階層には、管理者Ａがサービスを提供するためのサービス定義領域が設けられている。このサービス定義領域には、エリア定義領域＃０００００ｈのコード範囲である０００００ｈ乃至ＦＦＦＦｈのうち、０００８ｈが、サービスコードとして割り当てられている。ここで、サービスコード＃ｘｘｘｘｈのサービス定義領域を、以下、適宜、サービス定義領域＃ｘｘｘｘｈと記載する。

【００９４】

サービス定義領域＃０００８ｈの容量は８とされており、従って、８のユーザブロックで構成されるサービス領域の使用が可能となっている。また、サービス定義領域＃０００８ｈのサービスキーは、0101010101010101となっている。

【００９５】

さらに、管理者Ａのエリア定義領域＃００００ｈの階層には、管理者Ｂ１のエリア定義領域＃０１００ｈ、および管理者Ｂ２のエリア定義領域＃１０００ｈが

、その子の階層として設けられている。また、エリア定義領域＃００００ｈの階層には、図示せぬその他のエリア定義領域も設けられており、これにより、エリア定義領域＃００００ｈが使用可能なブロック数（空き容量）は、例えば、３７ブロックとなっている。

【００９６】

管理者Ｂ１のエリア定義領域＃０１００ｈのコード範囲としては、その親の階層であるエリア定義領域＃００００ｈのコード範囲である００００ｈ乃至ＦＦＦｈのうちの、０１００ｈ乃至０３ＦＦｈが割り当てられている。ここで、管理者Ｂ１のエリア定義領域のコード範囲が０１００ｈ乃至０３ＦＦｈであるため、その最小値である０１００ｈが、管理者Ｂ１のエリア定義領域のエリアコードとなっている。

【００９７】

また、エリア定義領域＃０１００ｈの空き容量またはエリアキーは、それぞれ、１４またはa0a0a0a0a0a0a0a0になっている。

【００９８】

さらに、管理者Ｂ１のエリア定義領域＃０１００ｈの階層には、管理者Ｃのエリア定義領域＃０３００ｈが、その子の階層として設けられている。そして、管理者Ｃのエリア定義領域＃０３００ｈのコード範囲としては、その親の階層であるエリア定義領域＃０１００ｈのコード範囲である０１００ｈ乃至０３ＦＦｈのうちの、０３００ｈ乃至０３ＦＦｈが割り当てられている。ここで、管理者Ｃのエリア定義領域のコード範囲が０３００ｈ乃至０３ＦＦｈであるため、その最小値である０３００ｈが、管理者Ｃのエリア定義領域のエリアコードとなっている。

【００９９】

また、エリア定義領域＃０３００ｈの空き容量またはエリアキーは、それぞれ、０またはb0b0b0b0b0b0b0b0になっている。

【０１００】

管理者Ｃのエリア定義領域＃０３００ｈの階層には、管理者Ｃがサービスを提供するためのサービス定義領域が設けられている。このサービス定義領域には、

エリア定義領域＃０３００ｈのコード範囲である０３００ｈ乃至０３ＦＦｈのうちの、０３０Ｃｈが、サービスコードとして割り当てられている。

【０１０１】

このサービスコード０３０Ｃｈが割り当てられているサービス定義領域、即ち、サービス定義領域＃０３０Ｃｈの容量は１６とされており、従って、１６のユーザブロックで構成されるサービス領域の使用が可能となっている。また、サービス定義領域＃０３０Ｃｈのサービスキーは、0202020202020202となっている。

【０１０２】

ここで、サービス定義領域＃０３０Ｃｈが管理するサービス領域の容量が１６であり、そのサービス定義領域＃０３０Ｃｈ自体が、１のブロックを、サービス定義ブロックとして使用することから、サービス定義領域＃０３０Ｃｈが存在することによって使用されるブロック数は１７（＝１６＋１）ブロックとなる。また、サービス定義領域＃０３０Ｃｈが属する階層のエリア定義領域＃０３００ｈが使用可能なブロック数は、その空き容量が０であるから、０ブロックである。さらに、エリア定義領域＃０３００ｈ自体が、１のブロックを、エリア定義ブロックとして使用する。従って、エリア定義領域＃０３００ｈの階層においては、使用されているブロックが１８（＝１７＋１）ブロックで、使用可能なブロックが０ブロックであるから、その親の階層（上位階層）であるエリア定義領域＃０１００ｈから割り当てられたブロック数が、１８（＝１８＋０）ブロックであることが分かる。

【０１０３】

さらに、エリア定義領域＃０１００ｈの階層については、その子の階層（下位階層）であるエリア定義領域＃０３００ｈで、上述のように、１８ブロックが使用されている。また、エリア定義領域＃０１００ｈ自体が１のブロックを、エリア定義ブロックとして使用している。そして、エリア定義領域＃０１００ｈの空き容量は、上述したように１４となっている。従って、エリア定義領域＃０１００ｈの階層においては、使用されているブロックが１９（＝１８＋１）ブロックで、使用可能なブロックが１４であるから、その親の階層であるエリア定義領域＃０００００ｈから割り当てられたブロックは、３３（＝１９＋１４）ブロックで

あることが分かる。

【０１０４】

一方、管理者Ｂ２のエリア定義領域＃１０００ｈのコード範囲としては、その親の階層であるエリア定義領域＃００００ｈのコード範囲である００００ｈ乃至ＦＦＦＦｈのうちの、１０００ｈ乃至１ＦＦＦｈが割り当てられている。ここで、管理者Ｂ２のエリア定義領域のコード範囲が１０００ｈ乃至１ＦＦＦｈであるため、その最小値である１０００ｈが、管理者Ｂ２のエリア定義領域のエリアコードとなっている。

【０１０５】

また、エリア定義領域＃１０００ｈの空き容量またはエリアキーは、それぞれ、４３またはc0c0c0c0c0c0c0c0になっている。

【０１０６】

管理者Ｂ２のエリア定義領域＃１０００ｈの階層には、管理者Ｂ２がサービスを提供するためのサービス定義領域が設けられている。このサービス定義領域には、エリア定義領域＃１０００ｈのコード範囲である１０００ｈ乃至１ＦＦＦｈのうちの、１０２２ｈが、サービスコードとして割り当てられている。

【０１０７】

このサービスコード１０２２ｈが割り当てられているサービス定義領域、即ち、サービス定義領域＃１０２２ｈの容量は４とされており、従って、４のユーザブロックで構成されるサービス領域の使用が可能となっている。また、サービス定義領域＃１０２２ｈのサービスキーは、0303030303030303となっている。

【０１０８】

ここで、サービス定義領域＃１０２２ｈが管理するサービス領域の容量が４であり、そのサービス定義領域＃１０２２ｈ自体が、１のブロックを、サービス定義ブロックとして使用することから、サービス定義領域＃１０２２ｈが存在することによって使用されるブロック数は５（＝４＋１）ブロックとなる。また、サービス定義領域＃１０２２ｈが属する階層のエリア定義領域＃１０００ｈが使用可能なブロック数は、その空き容量が４３であるから、４３ブロックである。さらに、エリア定義領域＃１０００ｈ自体が１のブロックを、エリア定義ブロック

として使用している。従って、エリア定義領域＃１０００ｈの階層においては、使用されているブロックが６（＝５＋１）ブロックで、使用可能なブロックが４３ブロックであるから、エリア定義領域＃１０００ｈに割り当てられたブロックは、４９（＝６＋４３）ブロックであることが分かる。

【０１０９】

以上のように、管理対象のエリア定義領域に割り当て可能な識別コードの範囲であるコード範囲をエリア定義領域に記憶させるようにしたので、そのコード範囲に基づき、管理対象のエリア定義領域を子の階層とし、そのエリア定義領域を管理するエリア定義領域を親の階層とする、図５に示したような階層構造を規定することができる。

【０１１０】

次に、図６を参照して、最上位階層のエリア定義領域＃００００ｈが割り当てられた管理者Ａが、例えば、ＩＣカード２の発行者であるとして、図５に示した階層構造が構成されていく過程について説明する。

【０１１１】

管理者Ａは、例えば、ユーザの要求に応じて、ＩＣカード２を発行する（１）。このＩＣカード２には、図５の階層構造のうち、例えば、エリア定義領域＃００００ｈだけが作成されている。

【０１１２】

そして、管理者Ａは、サービス定義領域＃０００８ｈによって管理されるサービス領域を利用して、所定のサービスの提供を開始する場合、そのサービス定義領域＃０００８ｈの作成を行うのに必要な情報を、発券機１０１に登録する（２）。

【０１１３】

ここで、発券機１０１は、例えば、図１のＲ／Ｗ１とコントローラ３から構成される。また、発券機１０１は、例えば、駅や、小売店、その他の施設などに設置することができる。

【０１１４】

その後、ユーザが、ＩＣカード２を、発券機１０１に装着すると（ＩＣカード

２を、発券機１０１が内蔵するＲ／Ｗ１との間で通信を行うことが可能な状態にすると）、発券機１０１は、発券作業を行い、即ち、登録された情報に基づいて、ＩＣカード２にコマンドおよび必要なデータを送信し、サービス定義領域＃０００８ｈを作成させる。これにより、ユーザは、サービス定義領域＃０００８ｈによって管理されるサービス領域を利用した、管理者Ａによるサービスの提供を受けることが可能となる。

【０１１５】

一方、管理者Ｂ１，Ｂ２それぞれは、ＩＣカード２を利用したサービスの提供を行いたい場合、管理者Ａとの間で契約を結び、管理者Ａに、エリア定義領域＃０１００ｈおよび＃１０００ｈの作成を行うのに必要な情報を、発券機１０１に登録してもらう（３），（４）。そして、ユーザが、ＩＣカード２を、発券機１０１に装着すると、発券機１０１は、発券作業を行い、即ち、登録された情報に基づいて、ＩＣカード２にコマンドおよび必要なデータを送信し、エリア定義領域＃０１００ｈおよび＃１０００ｈを作成させる。これにより、管理者Ｂ１またはＢ２は、エリア定義領域＃０１００ｈまたは＃１０００ｈにおいて定義されている範囲内において、ＩＣカード２のリソースを使用することが可能となる。なお、この場合、管理者Ｂ１，Ｂ２に対する発券業者は、管理者Ａということになる。

【０１１６】

その後、管理者Ｂ２が、サービス定義領域＃１０２２ｈによって管理されるサービス領域を利用して、所定のサービスの提供を開始する場合、そのサービス定義領域＃１０２２ｈの作成を行うのに必要な情報を、発券機１０１に登録する（５）。そして、ユーザが、ＩＣカード２を、発券機１０１に装着すると、発券機１０１は、登録された情報に基づいて、ＩＣカード２にコマンドおよび必要なデータを送信し、サービス定義領域＃１０２２ｈを作成させる。これにより、ユーザは、サービス定義領域＃１０２２ｈによって管理されるサービス領域を利用した、管理者Ｂ２によるサービスの提供を受けることが可能となる。

【０１１７】

また、管理者Ｃは、管理者Ｂ１の管理下において、ＩＣカード２を利用したサ

ービスの提供を行いたい場合、管理者Ｂ１との間で契約を結び、管理者Ｂ１に、エリア定義領域＃０３００ｈの作成を行うのに必要な情報を、発券機１０１に登録してもらう（6）。そして、ユーザが、ＩＣカード２を、発券機１０１に装着すると、発券機１０１は、登録された情報に基づいて、ＩＣカード２にコマンドおよび必要なデータを送信し、エリア定義領域＃０３００ｈを作成させる。これにより、管理者Ｃは、エリア定義領域＃０３００ｈにおいて定義されている範囲内において、ＩＣカード２のリソースを使用することが可能となる。なお、この場合、管理者Ｃに対する発券業者は、管理者Ｂ１ということになる。

【０１１８】

その後、管理者Ｃが、サービス定義領域＃０３０Ｃｈによって管理されるサービス領域を利用して、所定のサービスの提供を開始する場合、そのサービス定義領域＃０３０Ｃｈの作成を行うのに必要な情報を、発券機１０１に登録する（７）。そして、ユーザが、ＩＣカード２を、発券機１０１に装着すると、発券機１０１は、登録された情報に基づいて、ＩＣカード２にコマンドおよび必要なデータを送信し、サービス定義領域＃０３０Ｃｈを作成させる。これにより、ユーザは、サービス定義領域＃０３０Ｃｈによって管理されるサービス領域を利用した、管理者Ｃによるサービスの提供を受けることが可能となる。

【０１１９】

ＩＣカード２では、以上のように、発券機１０１からのコマンドにしたがって、エリア定義領域やサービス定義領域が作成される。このエリア定義領域を作成するエリア作成処理、およびサービス定義領域を作成するサービス作成処理は、例えば、シーケンサ９１によって行われるが、このエリア作成処理およびサービス作成処理について、図７および図８を参照して説明する。

【０１２０】

まず最初に、図７のフローチャートを参照して、エリア作成処理について説明する。

【０１２１】

ＩＣカード２が発券機１０１に装着されると、発券機１０１は、例えば、ＩＣカード２に対して、エリア定義領域を作成することを指令するコマンド（以下、

定義、エリア作成コマンドという）と、そのエリア定義領域を作成するために必要な情報、即ち、例えば、作成するエリア定義領域のコード範囲、そのエリア定義領域に割り当てられたブロック数（以下、適宜、割り当てブロック数という）、およびエリアキーなどを送信する。

【０１２２】

ＩＣカード２（シーケンサ９１）は、エリア作成コマンドを受信すると、それとともに送信されてくる作成対象のエリア定義領域のコード範囲、割り当てブロック数、およびエリアキーなどを認識する。さらに、ＩＣカード２では、作成対象のエリア定義領域のエリアコードを認識する。即ち、ここでは、作成対象のエリア定義領域のコード範囲の最小値が、そのエリアコードとして認識される。また、ＩＣカード２では、作成対象のエリア定義領域のコード範囲を含むコード範囲を有するエリア定義領域が、作成対象のエリア定義領域の親の階層のエリア定義領域として認識される。

【０１２３】

そして、ＩＣカード２では、ステップＳ１において、作成対象のエリア定義領域が、ＥＥＰＲＯＭ６６の中に既に作成されているかどうかが判定される。即ち、ステップＳ１では、作成対象のエリア定義領域のエリアコードと同一のエリアコードを有するエリア定義領域が、既に作成されているかどうかが判定される。

【０１２４】

ステップＳ１において、作成対象のエリア定義領域が既に作成されていると判定された場合、エリア作成処理を終了する。即ち、作成対象のエリア定義領域が既に作成されている場合は、同一のエリア定義領域を重複して作成する必要はないから、以降の処理は行われない。

【０１２５】

また、ステップＳ１において、作成対象のエリア定義領域が作成されていないと判定された場合、ステップＳ２に進み、作成対象のエリア定義領域のコード範囲および割り当てブロック数（容量）が適正かどうかが判定される。即ち、ステップＳ２では、作成対象のエリア定義領域のコード範囲が、親の階層のエリア定義領域に記憶されているコード範囲に含まれており、かつ作成対象のエリア定義

領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下であるかどうかが判定される。

【０１２６】

ステップＳ２において、作成対象のエリア定義領域のコード範囲および割り当てブロック数が適正でないと判定された場合、即ち、作成対象のエリア定義領域のコード範囲が、親の階層のエリア定義領域に記憶されているコード範囲に含まれていないか、または作成対象のエリア定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量を越えている場合、ステップＳ３に進み、エラー処理が行われ、エリア作成処理を終了する。即ち、ステップＳ３では、例えば、親の階層のエリア定義領域の子の階層として、エリア定義領域を作成することができない旨のメッセージが、発券機１０１に送信される。従って、この場合、エリア定義領域は作成されない（発券作業は行われない）。

【０１２７】

一方、ステップＳ２において、作成対象のエリア定義領域のコード範囲および割り当てブロック数が適正であると判定された場合、即ち、作成対象のエリア定義領域のコード範囲が、親の階層のエリア定義領域に記憶されているコード範囲に含まれおり、かつ作成対象のエリア定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下である場合、ステップＳ４に進み、作成対象のエリア定義領域が、親の階層のエリア定義領域の子の階層として作成される。

【０１２８】

即ち、ステップＳ４では、ＥＥＰＲＯＭ６６（図４）の中の空きブロックのうち、最も下のブロック（論理アドレスの最も大きい空きブロック）が、作成対象のエリア定義領域に対応するエリア定義ブロックとして確保される。さらに、そのエリア定義ブロックに、コード範囲、空き容量、エリアキーなどが書き込まれる（記憶される）。ここで、ステップＳ４では、コード範囲およびエリアキーとしては、発券機１０１から送信されてきたものが、そのまま書き込まれる。また、空き容量としては、発券機１０１から送信されてきた割り当てブロック数から１を減算した値が書き込まれる。なお、空き容量として、割り当てブロック数か

ら１を減算した値を書き込むのは、作成されたエリア定義領域が、１のブロックを使用するためである。

【０１２９】

その後、ステップＳ５に進み、親の階層のエリア定義領域の空き容量が書き換えられ、エリア作成処理を終了する。即ち、ステップＳ５では、親の階層のエリア定義領域の空き容量から、割り当てブロック数を減算した値が、その親の階層のエリア定義領域の空き容量として、新たに書き込まれる。

【０１３０】

図５に示した管理者Ｂ１，Ｂ２，Ｃそれぞれのエリア定義領域＃０１００ｈ，＃１０００ｈ，＃０３００ｈは、以上のエリア作成処理が行われることで作成される。

【０１３１】

即ち、ＩＣカード２の発行時において、その発行者でもある管理者Ａが、ＩＣカード２のリソースすべてを有しており、ＩＣカード２の使用可能な識別コードまたは容量が、例えば、０００００ｈ乃至ＦＦＦＦｈまたは６５５３３ブロックであるとすると、ＩＣカード２の発行時においては、エリア定義領域としては、コード範囲が０００００ｈ乃至ＦＦＦＦｈで、空き容量が６５５３２となっている、最上位階層のエリア定義領域＃００００ｈだけが存在している。

【０１３２】

なお、本実施の形態では、図４に示したように、ＥＥＰＲＯＭ６６は、６５５３６のブロックを有しているが、発行直後のＩＣカード２において、使用可能な容量が、それより３ブロック少ない６５５３３ブロックであるのは、図４に示したように、製造ＩＤブロック、発行ＩＤブロック、システム定義ブロックが存在するためである。

【０１３３】

また、最上位階層のエリア定義領域＃００００ｈの空き容量が、使用可能な容量である６５５３３ブロックより１ブロック少ない６５５３２ブロックとなるのは、エリア定義領域＃００００ｈ自体が、１ブロックを使用するためである。

【０１３４】

管理者Ａが、自身のリソースのうち、例えば、０１００ｈ乃至０３ＦＦｈの範囲の識別コードと、３３ブロックを、管理者Ｂ１に分け与える場合には、エリア作成処理が行われることにより、エリア定義領域＃０１００ｈが作成される。即ち、この場合、０１００ｈ乃至０３ＦＦｈがコード範囲として、また、３２ブロックが空き容量として、エリア定義領域＃０１００ｈに書き込まれる。なお、空き容量が、管理者Ａから分け与えられる３３ブロックより１ブロック少ないのは、エリア定義領域＃０１００ｈ自体が、１ブロックを使用するからである。

【０１３５】

エリア定義領域＃０１００ｈが作成されると、管理者Ａのエリア定義領域＃００００ｈの空き容量は、管理者Ｂ１に分け与えた３３ブロックだけ減らされる。

【０１３６】

また、管理者Ａが、自身のリソースのうち、例えば、１０００ｈ乃至１ＦＦＦｈの範囲の識別コードと、４９ブロックを、管理者Ｂ２に分け与える場合には、エリア作成処理が行われることにより、エリア定義領域＃１０００ｈが作成される。即ち、この場合、１０００ｈ乃至１ＦＦＦｈがコード範囲として、また、４８ブロックが空き容量として、エリア定義領域＃１０００ｈに書き込まれる。なお、空き容量が、管理者Ａから分け与えられる４９ブロックより１ブロック少ないのは、エリア定義領域＃１０００ｈ自体が、１ブロックを使用するからである。

【０１３７】

エリア定義領域＃１０００ｈが作成されると、管理者Ａのエリア定義領域＃００００ｈの空き容量は、管理者Ｂ２に分け与えた３３ブロックだけ減らされる。

【０１３８】

管理者Ｂ１またはＢ２それぞれは、以上のようにして、エリア定義領域＃０１００ｈまたは＃１０００ｈが作成されると、そのエリア定義領域＃０１００ｈまたは＃１０００ｈの階層に、その子の階層としてのエリア定義領域や、サービス定義領域を作成することが可能となる。

【０１３９】

例えば、いま、管理者Ｂ１が、自身のリソースのうち、例えば、０３００ｈ乃至０３ＦＦｈの範囲の識別コードと、１８ブロックを、管理者Ｃに分け与える場合には、エリア作成処理が行われることにより、エリア定義領域＃０３００ｈが作成される。即ち、この場合、０３００ｈ乃至０３ＦＦｈがコード範囲として、また、１７ブロックが空き容量として、エリア定義領域＃０３００ｈに書き込まれる。なお、空き容量が、管理者Ｂ１から分け与えられる１８ブロックより１ブロック少ないのは、エリア定義領域＃０３００ｈ自体が、１ブロックを使用するからである。

【０１４０】

エリア定義領域＃０３００ｈが作成されると、管理者Ｂ１エリア定義領域＃０１００ｈの空き容量は、管理者Ｃに分け与えた１８ブロックだけ減らされる。即ち、上述したように、エリア定義領域＃０１００ｈが作成された時点では、その空き領域は、３２ブロックであったが、１８ブロックだけ減らされて、図５に示したように、１４ブロックとなる。

【０１４１】

次に、図８のフローチャートを参照して、サービス作成処理について説明する。

【０１４２】

ＩＣカード２が発券機１０１に装着されると、発券機１０１は、ＩＣカード２に対して、サービス定義領域を作成することを指令するコマンド（以下、定義、サービス作成コマンドという）と、そのサービス定義領域を作成するために必要な情報、即ち、例えば、作成するサービス定義領域のサービスコード、そのサービス定義領域に割り当てられたブロック数（これも、以下、適宜、割り当てブロック数という）、およびサービスキーなどを送信する。

【０１４３】

ＩＣカード２（シーケンサ９１）は、サービス作成コマンドを受信すると、それとともに送信されてくる作成対象のサービス定義領域のサービスコード、割り当てブロック数、およびサービスキーなどを認識する。さらに、ＩＣカード２で

は、作成対象のサービス定義領域のサービスコードを含むコード範囲を有するエリア定義領域が、作成対象のサービス定義領域の親の階層のエリア定義領域として認識される。

【０１４４】

そして、ＩＣカード２では、ステップＳ１１において、作成対象のサービス定義領域が、ＥＥＰＲＯＭ６６の中に既に作成されているかどうかが判定される。即ち、ステップＳ１１では、作成対象のサービス定義領域のサービスコードと同一のサービスコードを有するサービス定義領域が、既に作成されているかどうかが判定される。

【０１４５】

ステップＳ１１において、作成対象のサービス定義領域が既に作成されていると判定された場合、サービス作成処理を終了する。即ち、作成対象のサービス定義領域が既に作成されている場合は、同一のサービス定義領域を重複して作成する必要はないから、以降の処理は行われない。

【０１４６】

また、ステップＳ１１において、作成対象のサービス定義領域が作成されていないと判定された場合、ステップＳ１２に進み、作成対象のサービス定義領域のサービスコードおよび割り当てブロック数（容量）が適正かどうかが判定される。即ち、ステップＳ１２では、作成対象のサービス定義領域のサービスコードが、親の階層のエリア定義領域に記憶されているコード範囲に含まれており、かつ作成対象のサービス定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下であるかどうかが判定される。

【０１４７】

ステップＳ１２において、作成対象のサービス定義領域のサービスコードおよび割り当てブロック数が適正でないと判定された場合、即ち、作成対象のサービス定義領域のサービスコードが、親の階層のエリア定義領域に記憶されているコード範囲に含まれていないか、または作成対象のサービス定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量を越えている場合、ステップＳ１３に進み、エラー処理が行われ、エリア作成処理を終了する

。即ち、ステップＳ３では、例えば、親の階層のエリア定義領域の階層に、サービス定義領域を作成することができない旨のメッセージが、発券機１０１に送信される。従って、この場合、サービス定義領域は作成されない。

【０１４８】

一方、ステップＳ１２において、作成対象のサービス定義領域のサービスコードおよび割り当てブロック数が適正であると判定された場合、即ち、作成対象のサービス定義領域のサービスコードが、親の階層のエリア定義領域に記憶されているコード範囲に含まれおり、かつ作成対象のサービス定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下である場合、ステップＳ１４に進み、作成対象のサービス定義領域が、親の階層のエリア定義領域の階層に作成される。

【０１４９】

即ち、ステップＳ１４では、ＥＥＰＲＯＭ６６（図４）の中の空きブロックのうち、最も下のブロック（論理アドレスの最も大きい空きブロック）が、作成対象のサービス定義領域に対応するサービス定義ブロックとして確保される。さらに、そのサービス定義ブロックに、サービスコード、容量、サービスキーなどが書き込まれる。ここで、ステップＳ１４では、サービスコードおよびサービスキーとしては、発券機１０１から送信されてきたものが、そのまま書き込まれる。また、容量としては、発券機１０１から送信されてきた割り当てブロック数から１を減算した値が書き込まれる。なお、容量として、割り当てブロック数から１を減算した値を書き込むのは、作成されたサービス定義領域が、１のブロックを使用するためである。

【０１５０】

また、ステップＳ１４では、作成されたサービス定義領域に書き込まれた容量に対応する数の空きブロックが、論理アドレスの小さい順に選択され、そのサービス定義領域が管理するサービス領域を構成するユーザブロックとして確保され、ステップＳ１５に進む。

【０１５１】

ステップＳ１５では、親の階層のエリア定義領域の空き容量が書き換えられ、

サービス作成処理を終了する。即ち、ステップＳ１５では、親の階層のエリア定義領域の空き容量から、割り当てブロック数を減算した値が、そのエリア定義領域の空き容量として、新たに書き込まれる。

【０１５２】

図５に示した管理者Ａ，Ｂ２，Ｃそれぞれのサービス定義領域＃０００８ｈ，＃１０２２ｈ，＃０３０Ｃｈは、以上のサービス作成処理が行われることで作成される。

【０１５３】

即ち、管理者Ａが、自身のリソースのうち、例えば、０００８ｈの識別コードと、９ブロックの容量を用いてサービスの提供を行う場合には、サービス作成処理が行われることにより、サービス定義領域＃０００８ｈが作成され、そこに、容量として、８ブロックが書き込まれる。さらに、８個の空きブロックがユーザブロックとして確保され、エリア定義領域＃０００８ｈによって管理されるサービス領域とされる。なお、サービス定義領域＃０００８ｈに書き込まれる容量が、９ブロックより１ブロック少ないのは、サービス定義領域＃０００８ｈ自体が、１ブロックを使用するからである。

【０１５４】

サービス定義領域＃０００８ｈが作成されると、管理者Ａのエリア定義領域＃００００ｈの空き容量は、サービス定義領域＃０００８ｈに分け与えた９ブロックだけ減らされる。

【０１５５】

以上により、管理者Ａは、サービス定義領域＃０００８ｈで管理される８ブロックのサービス領域を用いて、サービスを提供することが可能となる。

【０１５６】

また、管理者Ｂ２が、自身のリソースのうち、例えば、１０２２ｈの識別コードと、５ブロックの容量を用いてサービスの提供を行う場合には、サービス作成処理が行われることにより、サービス定義領域＃１０２２ｈが作成され、そこに、容量として、４ブロックが書き込まれる。さらに、４個の空きブロックがユーザブロックとして確保され、エリア定義領域＃１０２２ｈによって管理されるサ

ービス領域とされる。なお、サービス定義領域＃１０２２ｈに書き込まれる容量が、５ブロックより１ブロック少ないのは、サービス定義領域＃１０２２ｈ自体が、１ブロックを使用するからである。

【０１５７】

サービス定義領域＃１０２２ｈが作成されると、管理者Ｂ２のエリア定義領域＃１０００ｈの空き容量は、サービス定義領域＃１０２２ｈに分け与えた５ブロックだけ減らされる。即ち、上述したように、エリア定義領域＃１０００ｈが作成された時点では、その空き容量は、４８ブロックであったが、５ブロックだけ減らされて、図５に示したように、４３ブロックとなる。

【０１５８】

以上により、管理者Ｂ２は、サービス定義領域＃１０２２ｈで管理される４ブロックのサービス領域を用いて、サービスを提供することが可能となる。

【０１５９】

さらに、管理者Ｃが、自身のリソースのうち、例えば、０３０Ｃｈの識別コードと、１７ブロックの容量を用いてサービスの提供を行う場合には、サービス作成処理が行われることにより、サービス定義領域＃０３０Ｃｈが作成され、そこに、容量として、１６ブロックが書き込まれる。さらに、１６個の空きブロックがユーザブロックとして確保され、エリア定義領域＃０３０Ｃｈによって管理されるサービス領域とされる。なお、サービス定義領域＃０３０Ｃｈに書き込まれる容量が、１７ブロックより１ブロック少ないのは、サービス定義領域＃０３０Ｃｈ自体が、１ブロックを使用するからである。

【０１６０】

サービス定義領域＃０３０Ｃｈが作成されると、管理者Ｃのエリア定義領域＃０３００ｈの空き容量は、サービス定義領域＃０３０Ｃｈに分け与えた１７ブロックだけ減らされる。即ち、上述したように、エリア定義領域＃０３００ｈが作成された時点では、その空き容量は、１７ブロックであったが、１７ブロックだけ減らされて、図５に示したように、０ブロックとなる。

【０１６１】

以上により、管理者Ｃは、サービス定義領域＃０３０Ｃｈで管理される１６ブ

ロックのサービス領域を用いて、サービスを提供することが可能となる。

【０１６２】

以上のように、コード範囲および空き容量を記憶しているエリア定義領域に基づいて、ＥＥＰＲＯＭ６６を管理するようにしたので、ＩＣカード２のリソース管理を行うことが可能となる。即ち、あるエリア定義領域の階層の中で使用可能な容量および識別コードを制限することができる。その結果、例えば、ある管理者が、自身に割り当てられたリソース（ここでは、使用可能な容量および識別コード）の一部を、他の管理者に分け与えて、ＩＣカード２を共有したとしても、識別コードが、異なる管理者の間で重複することや、管理者が、あらかじめ、契約等で定められた容量を超えてＥＥＰＲＯＭ６６を使用することなどを防止することができる。

【０１６３】

次に、ＩＣカード２では、図５で説明したように、ＥＥＰＲＯＭ６６の記憶領域が、エリア定義領域を階層とする階層構造をなしており、さらに、各エリア定義領域およびサービス定義領域に、認証のためのキー（本実施の形態では、エリア定義領域またはサービス定義領域のキーを、それぞれエリアキーまたはサービスキーと呼んでいる）が記憶されている結果、ＩＣカード２に対するフレキシブルでセキュリティの高いアクセス制御を行うことが可能となっている。

【０１６４】

即ち、管理者どうしの間において、例えば、図９に示すような情報のやりとりを行うことで、ＩＣカード２に対するフレキシブルでセキュリティの高いアクセス制御を実現することができる。

【０１６５】

具体的には、ＩＣカード２の発行者でもある管理者Ａは、ＥＥＰＲＯＭ６６（図４）のシステム定義ブロックに記憶させるシステムキーと、自身のエリア定義領域＃００００ｈのエリアキーを決定し、システムキーをシステム定義ブロックに、エリアキー＃００００ｈをエリア定義領域＃００００ｈに、それぞれ記憶させておく。ここで、エリア定義領域＃ｘｘｘｘｈのエリアキーを、以下、適宜、エリアキー＃ｘｘｘｘｈと記載する。

【０１６６】

さらに、管理者Ａは、システムキーを、エリアキー＃００００ｈで暗号化し、エリア中間キーK_Aを生成しておく。なお、暗号化の手法としては、例えば、ＤＥＳ（Data Encryption Standard）や、ＦＥＡＬ（Fast Data Encipherment Algolithm）などを採用することができる。

【０１６７】

そして、管理者Ａは、自身のリソースを、管理者Ｂ１に分け与えるとき、エリア中間キーK_Aを、管理者Ｂ１に与える。さらに、管理者Ａは、管理者Ｂ１のエリアキー＃０１００ｈを決定し、自身のエリアコード＃００００ｈとともに、管理者Ｂ１に与える（配布する）。

【０１６８】

従って、管理者Ｂ１は、エリア中間キーK_Aおよび自身のエリアキー＃０１００ｈを認識することができるが、システムキー、および、いわば親である管理者Ａのエリアキー＃００００ｈは認識することができない。但し、管理者Ｂ１のエリアキー＃０１００ｈは、親である管理者Ａが、いわば子である管理者Ｂ１に与えたものであるから、親である管理者Ａは、子である管理者Ｂ１のエリアキー＃０１００ｈを認識している。

【０１６９】

なお、管理者Ａが管理者Ｂ１に与えたエリアキー＃０１００ｈは、管理者Ｂ１のエリア定義領域＃０１００ｈのエリア作成処理（図７）において、そのエリア定義領域＃０１００ｈに書き込まれる。

【０１７０】

管理者Ｂ１は、その親である管理者Ａから得たエリア中間キーK_Aを、やはり管理者Ａから得たエリアキー＃０１００ｈで暗号化し、エリア中間キーK_{B1}を生成しておく。

【０１７１】

また、管理者Ａは、自身のリソースを、管理者Ｂ２に分け与えるときも、エリア中間キーK_Aを、管理者Ｂ２に与える。さらに、管理者Ａは、管理者Ｂ２のエリアキー＃１０００ｈを決定し、自身のエリアコード＃００００ｈとともに、管

理者Ｂ２に与える。

【０１７２】

従って、管理者Ｂ２は、エリア中間キーK_Aおよび自身のエリアキー＃１０００ｈを認識することができるが、システムキー、および親である管理者Ａのエリアキー＃００００ｈは認識することができない。但し、管理者Ｂ２のエリアキー＃１０００ｈは、親である管理者Ａが、子である管理者Ｂ２に与えたものであるから、親である管理者Ａは、子である管理者Ｂ２のエリアキー＃１０００ｈを認識している。

【０１７３】

なお、管理者Ａが管理者Ｂ２に与えたエリアキー＃１０００ｈは、管理者Ｂ２のエリア定義領域＃１０００ｈのエリア作成処理において、そのエリア定義領域＃１０００ｈに書き込まれる。

【０１７４】

管理者Ｂ２は、その親である管理者Ａから得たエリア中間キーK_Aを、やはり管理者Ａから得たエリアキー＃１０００ｈで暗号化し、エリア中間キーK_{B2}を生成しておく。

【０１７５】

一方、管理者Ｂ１は、自身のリソースを、管理者Ｃに分け与えるとき、エリア中間キーK_{B1}を、管理者Ｃに与える。さらに、管理者Ｂ１は、管理者Ｃのエリアキー＃０３００ｈを決定し、自身のエリアコード＃０１００ｈおよび親である管理者Ａのエリアコード＃００００ｈとともに、管理者Ｃに与える。

【０１７６】

従って、管理者Ｃは、エリア中間キーK_{B1}および自身のエリアキー＃０３００ｈを認識することができるが、親である管理者Ｂ１のエリアキー＃０１００ｈは認識することができない。但し、エリアキー＃０１００ｈは、親である管理者Ｂ１が、子である管理者Ｃに与えたものであるから、親である管理者Ｂ１は、子である管理者Ｃのエリアキー＃０３００ｈを認識している。

【０１７７】

なお、管理者Ｂ１が管理者Ｃに与えたエリアキー＃０３００ｈは、管理者Ｃの

エリア定義領域＃０３００ｈのエリア作成処理において、そのエリア定義領域＃０３００ｈに書き込まれる。

【０１７８】

管理者Ｃは、その親である管理者Ｂ１から得たエリア中間キーK_{B1}を、やはり管理者Ｂ１から得たエリアキー＃０３００ｈで暗号化し、エリア中間キーK_Cを生成しておく。

【０１７９】

そして、管理者Ａは、自身のエリア定義領域＃００００ｈの階層に作成されたサービス定義領域＃０００８ｈで管理されるサービス領域を利用してサービスを提供するとき、図１０に示すように、サービス定義領域＃０００８ｈに記憶させたサービスキー（サービス定義領域＃ｘｘｘｘｈに記憶されたサービスキーを、以下、適宜、サービスキー＃ｘｘｘｘｈと記載する）を、エリア中間キーK_Aで暗号化し、サービス中間キー$K_{\#0008h}$を生成して、エリア中間キーK_Aとともに、サービス提供装置１１１に登録する。さらに、管理者Ａは、自身のエリア定義領域＃００００ｈのエリアコード＃００００ｈと、そのエリア定義領域＃００００ｈの階層に作成されたサービス定義領域＃０００８ｈのサービスコード＃０００８ｈも、サービス提供装置１１１に登録する。

【０１８０】

ここで、サービス提供装置１１１は、例えば、図１のＲ／Ｗ１とコントローラ３から構成され、所定のサービス領域に対してデータを読み書きすることで、所定のサービスを提供するようになされている。

【０１８１】

この場合、サービス提供装置１１１に、ＩＣカード２が装着されると、サービス提供装置１１１とＩＣカード２との間で、次のようにして相互認証が行われる。

【０１８２】

即ち、サービス提供装置１１１は、図１１に示すように、登録されているエリアコード＃００００ｈと、サービスコード＃０００８ｈとを、ＩＣカード２に送信する。ＩＣカード２（シーケンサ９１）では、サービス提供装置１１１からの

エリアコード＃０００００ｈおよびサービスコード＃０００８ｈが受信される。

【０１８３】

そして、ＩＣカード２では、システム定義ブロック（図４）に記憶されているシステムキーが読み出されるとともに、サービス提供装置１１１から受信したエリアコード＃０００００ｈを有するエリア定義領域からエリアキー＃０００００ｈが読み出される。さらに、システムキーが、エリアキー＃０００００ｈで暗号化され、その結果、図１０のサービス提供装置１１１に登録されているエリア中間キーK_Aと同一のキーが生成される。このエリア中間キーK_Aと同一のキーは、認証に用いる第１アクセスキー（認証キー）K_{bc}とされる。

【０１８４】

また、ＩＣカード２では、サービス提供装置１１１から受信したサービスコード＃０００８ｈを有するサービス定義領域からサービスキー＃０００８ｈが読み出される。そして、そのサービスキー＃０００８ｈで、エリア中間キーK_Aが暗号化され、その結果、図１０のサービス提供装置１１１に登録されているサービス中間キー$K_{\#0008h}$と同一のキーが生成される。このサービス中間キー$K_{\#0008h}$と同一のキーは、認証に用いる第２アクセスキーK_{ac}とされる。

【０１８５】

従って、いまの場合、サービス提供装置１１１には、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_Aまたはサービス中間キー$K_{\#0008h}$が登録されており、ＩＣカード２では、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_Aまたはサービス中間キー$K_{\#0008h}$が生成される。

【０１８６】

そして、サービス提供装置１１１は、例えば、図１２に示すようにして、ＩＣカード２の認証を行う。

【０１８７】

即ち、サービス提供装置１１１では、乱数が発生され、その乱数が、アルゴリズムＥ１にしたがって変換される。即ち、乱数が、第２アクセスキーK_{ac}で暗号化（例えば、ＤＥＳ暗号化）され、その暗号化結果が、第１アクセスキーK_{bc}で

復号（例えば、ＤＥＳ復号）される。さらに、その復号結果が、第２アクセスキーK_{ac}で暗号化される。アルゴリズムＥ１による乱数の変換結果は、ＩＣカード２に送信される。

【０１８８】

ＩＣカード２では、サービス提供装置１１１からのアルゴリズムＥ１による乱数の変換結果が、アルゴルズムＤ１にしたがって変換される。即ち、アルゴリズムＥ１による変換結果が、第２アクセスキーK_{ac}で復号され、その復号結果が、第１アクセスキーK_{bc}で暗号化される。さらに、その暗号化結果が、第２アクセスキーK_{ac}で復号される。

【０１８９】

そして、ＩＣカード２では、アルゴリズムＤ１による変換結果が、さらに、アルゴリズムＥ２にしたがって変換される。即ち、アルゴリズムＤ１による変換結果が、第１アクセスキーK_{bc}で暗号化される一方、第１アクセスキーK_{bc}が、第２アクセスキーK_{ac}で暗号化される。そして、アルゴリズムＤ１による変換結果の、第１アクセスキーK_{bc}での暗号化結果が、第１アクセスキーK_{bc}の、第２アクセスキーK_{ac}での暗号化結果で復号される。さらに、その復号結果が、第１アクセスキーK_{bc}で暗号化され、サービス提供装置１１１に送信される。

【０１９０】

サービス提供装置１１１では、ＩＣカード２からのアルゴリズムＥ２による変換結果が、アルゴリズムＤ２にしたがって変換される。即ち、アルゴリズムＥ２による変換結果が、第１アクセスキーK_{bc}で復号される一方、第１アクセスキーK_{bc}が、第２アクセスキーK_{ac}で暗号化される。そして、アルゴリズムＥ２による変換結果の、第１アクセスキーK_{bc}での復号結果が、第１アクセスキーK_{bc}の、第２アクセスキーK_{ac}での暗号化結果で暗号化される。さらに、その暗号化結果が、第１アクセスキーK_{bc}で復号される。

【０１９１】

そして、サービス提供装置１１１では、元の乱数と、アルゴリズムＤ２による変換結果とを比較することで、ＩＣカード２の認証を行う。即ち、元の乱数と、アルゴリズムＤ２による変換結果とが一致している場合は、ＩＣカード２が適正

なものとして認識され、一致していない場合は、ＩＣカード２が不適正なもの（例えば、偽造されたもの）として認識される。

【０１９２】

ＩＣカード２が適正なものとして認識されると、ＩＣカード２において、例えば、図１３に示すようにして、サービス提供装置１１１の認証が行われる。

【０１９３】

即ち、ＩＣカード２では、乱数が発生され、その乱数が、アルゴリズムＥ２にしたがって変換され、サービス提供装置１１１に送信される。

【０１９４】

サービス提供装置１１１では、ＩＣカード２からのアルゴリズムＥ２による乱数の変換結果が、アルゴルズムＤ２にしたがって変換される。さらに、そのアルゴリズムＤ２による変換結果が、アルゴリズムＥ１にしたがって変換され、ＩＣカード２に送信される。

【０１９５】

ＩＣカード２では、サービス提供装置１１１からのアルゴリズムＥ１による変換結果が、アルゴリズムＤ１にしたがって変換され、その変換結果と、元の乱数とを比較することで、サービス提供装置１１１の認証が行われる。即ち、元の乱数と、アルゴリズムＤ２による変換結果とが一致している場合は、サービス提供装置１１１が適正なものとして認識され、一致していない場合は、サービス提供装置１１１が不適正なもの（例えば、改造されたもの）として認識される。

【０１９６】

ＩＣカード２およびサービス提供装置１１１のいずれも適正なものと認められた場合、ＩＣカード２では、サービス提供装置１１１から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図１０および図１１で説明した場合においては、サービス定義領域＃０００８ｈで管理されているサービス領域のみへのアクセスが可能となる。

【０１９７】

即ち、エリア中間キーK_A、エリアコード＃０００００ｈ、サービスキー＃００

０８ｈ、およびサービスコード＃０００８ｈを知っている管理者Ａは、サービス定義領域＃０００８ｈで管理されているサービス領域にアクセスすることができる。但し、管理者Ａは、サービスキー＃１０２２ｈや＃０３０Ｃｈを知らないから、基本的に、サービス定義領域＃１０２２ｈや＃０３０Ｃｈで管理されているサービス領域にアクセスすることはできない。

【０１９８】

次に、管理者Ｂ２が、自身のエリア定義領域＃１０００ｈの階層に作成されたサービス定義領域＃１０２２ｈで管理されるサービス領域を利用してサービスを提供するときは、図１４に示すように、サービス定義領域＃１０２２ｈに記憶させたサービスキー＃１０２２ｈを、エリア中間キーK_{B2}で暗号化し、サービス中間キー$K_{\#1022h}$を生成して、エリア中間キーK_{B2}とともに、サービス提供装置１１１に登録する。そして、管理者Ｂ２は、自身のエリア定義領域＃１０００ｈの階層より上位の階層のエリア定義領域のエリアコード、即ち、いまの場合、管理者Ａのエリア定義領域＃００００ｈのエリアコード＃００００ｈ、および自身のエリア定義領域＃１０００ｈのエリアコード＃１０００ｈと、そのエリア定義領域＃１０００ｈの階層に作成されたサービス定義領域＃１０２２ｈのサービスコード＃１０２２ｈも、サービス提供装置１１１に登録する。

【０１９９】

この場合、サービス提供装置１１１に、ＩＣカード２が装着されると、サービス提供装置１１１とＩＣカード２との間で、次のようにして相互認証が行われる。

【０２００】

即ち、サービス提供装置１１１は、図１５に示すように、登録されているエリアコード＃００００ｈおよび＃１０００ｈと、サービスコード＃１０２２ｈとを、ＩＣカード２に送信する。ＩＣカード２（シーケンサ９１）では、サービス提供装置１１１からのエリアコード＃００００ｈおよび＃１０００ｈ、並びにサービスコード＃１０２２ｈが受信される。

【０２０１】

そして、ＩＣカード２では、システム定義ブロック（図４）に記憶されている

システムキーが読み出されるとともに、サービス提供装置１１１から受信したエリアコード＃００００ｈまたは＃１０００ｈを有するエリア定義領域それぞれからエリアキー＃００００ｈまたは＃１０００ｈが読み出される。さらに、システムキーが、エリアキー＃００００ｈで暗号化され、その結果、エリア中間キーK_Aと同一のキーが生成される。そして、そのエリア中間キーK_Aと同一のキーが、エリアキー＃１０００ｈで暗号化され、その結果、図１４のサービス提供装置１１１に登録されているエリア中間キーK_{B2}と同一のキーが生成される。このエリア中間キーK_{B2}と同一のキーは、認証に用いる第１アクセスキーK_{bc}とされる。

【０２０２】

また、ＩＣカード２では、サービス提供装置１１１から受信したサービスコード＃１０２２ｈを有するサービス定義領域からサービスキー＃１０２２ｈが読み出される。そして、そのサービスキー＃１０２２ｈで、エリア中間キーK_{B2}と同一のキーが暗号化され、その結果、図１４のサービス提供装置１１１に登録されているサービス中間キー$K_{\#1022h}$と同一のキーが生成される。このサービス中間キー$K_{\#1022h}$と同一のキーは、認証に用いる第２アクセスキーK_{ac}とされる。

【０２０３】

従って、いまの場合、サービス提供装置１１１には、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_{B2}またはサービス中間キー$K_{\#1022h}$が登録されており、ＩＣカード２では、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_{B2}またはサービス中間キー$K_{\#1022h}$が生成される。

【０２０４】

そして、ＩＣカード２およびサービス提供装置１１１の間で、図１２および図１３で説明した場合と同様にして、相互認証が行われる。

【０２０５】

その相互認証の結果、ＩＣカード２およびサービス提供装置１１１のいずれも適正なものと認められた場合、ＩＣカード２では、サービス提供装置１１１から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図１４および図１５で

説明した場合においては、サービス定義領域＃１０２２ｈで管理されているサービス領域のみへのアクセスが可能となる。

【０２０６】

即ち、エリア中間キーK_{B2}、エリアコード＃０００００ｈ、＃１０００ｈ、サービスキー＃１０２２ｈ、並びにサービスコード＃１０２２ｈを知っている管理者Ｂ２は、サービス定義領域＃１０２２ｈで管理されているサービス領域にアクセスすることができる。但し、管理者Ｂ２は、サービスキー＃０００８ｈや＃０３０Ｃｈを知らないから、基本的に、サービス定義領域＃０００８ｈや＃０３０Ｃｈで管理されているサービス領域にアクセスすることはできない。

【０２０７】

次に、管理者Ｃが、自身のエリア定義領域＃０３００ｈの階層に作成されたサービス定義領域＃０３０Ｃｈで管理されるサービス領域を利用してサービスを提供するときは、図１６に示すように、サービス定義領域＃０３０Ｃｈに記憶させたサービスキー＃０３０Ｃｈを、エリア中間キーK_Cで暗号化し、サービス中間キー$K_{\#030Ch}$を生成して、エリア中間キーK_Cとともに、サービス提供装置１１１に登録する。そして、管理者Ｃは、自身のエリア定義領域＃０３００ｈの階層より上位の階層のエリア定義領域のエリアコード、即ち、いまの場合、管理者Ａのエリア定義領域＃００００ｈのエリアコード＃００００ｈおよび管理者Ｂ１のエリア定義領域＃０１００ｈのエリアコード０１００ｈ、並びに自身のエリア定義領域＃０３００ｈのエリアコード＃０３００ｈと、そのエリア定義領域＃０３００ｈの階層に作成されたサービス定義領域＃０３０Ｃｈのサービスコード＃０３０Ｃｈも、サービス提供装置１１１に登録する。

【０２０８】

この場合、サービス提供装置１１１に、ＩＣカード２が装着されると、サービス提供装置１１１とＩＣカード２との間で、次のようにして相互認証が行われる。

【０２０９】

即ち、サービス提供装置１１１は、図１７に示すように、登録されているエリアコード＃００００ｈ、＃０１００ｈ、および＃０３００ｈと、サービスコード

＃０３０Ｃｈとを、ＩＣカード２に送信する。ＩＣカード２（シーケンサ９１）では、サービス提供装置１１１からのエリアコード＃００００ｈ、＃０１００ｈ、および＃０３００ｈ、並びにサービスコード＃０３０Ｃｈが受信される。

【０２１０】

そして、ＩＣカード２では、システム定義ブロック（図４）に記憶されているシステムキーが読み出されるとともに、サービス提供装置１１１から受信したエリアコード＃００００ｈ、＃０１００ｈ、または＃０３００ｈを有するエリア定義領域それぞれからエリアキー＃００００ｈ、＃０１００ｈ、または＃０３００ｈが読み出される。さらに、システムキーが、エリアキー＃００００ｈで暗号化され、その結果、エリア中間キーK_Aと同一のキーが生成される。また、そのエリア中間キーK_Aと同一のキーが、エリアキー＃０１００ｈで暗号化され、その結果、エリア中間キーK_{B1}と同一のキーが生成される。そして、そのエリア中間キーK_{B1}と同一のキーが、エリアキー＃０３００ｈで暗号化され、その結果、図１６のサービス提供装置１１１に登録されているエリア中間キーK_Cと同一のキーが生成される。このエリア中間キーK_Cと同一のキーは、認証に用いる第１アクセスキーK_{bc}とされる。

【０２１１】

また、ＩＣカード２では、サービス提供装置１１１から受信したサービスコード＃０３０Ｃｈを有するサービス定義領域からサービスキー＃０３０Ｃｈが読み出される。そして、そのサービスキー＃０３０Ｃｈで、エリア中間キーK_Cが暗号化され、その結果、図１６のサービス提供装置１１１に登録されているサービス中間キー$K_{\#030Ch}$と同一のキーが生成される。このサービス中間キー$K_{\#030Ch}$と同一のキーは、認証に用いる第２アクセスキーK_{ac}とされる。

【０２１２】

従って、いまの場合、サービス提供装置１１１には、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_Cまたはサービス中間キー$K_{\#030Ch}$がそれぞれ登録されており、ＩＣカード２では、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_Cまたはサービス中間キー$K_{\#030Ch}$がそれぞれ生成される。

【０２１３】

そして、ＩＣカード２およびサービス提供装置１１１の間で、図１２および図１３で説明した場合と同様にして、相互認証が行われる。

【０２１４】

その相互認証の結果、ＩＣカード２およびサービス提供装置１１１のいずれも適正なものと認められた場合、ＩＣカード２では、サービス提供装置１１１から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図１６および図１７で説明した場合においては、サービス定義領域＃０３０Ｃｈで管理されているサービス領域のみへのアクセスが可能となる。

【０２１５】

即ち、エリア中間キーK_C、エリアコード＃０００００ｈ、＃０１００ｈ、＃０３００ｈ、サービスキー＃０３０Ｃｈ、並びにサービスコード＃０３０Ｃｈを知っている管理者Ｃは、サービス定義領域＃０３０Ｃｈで管理されているサービス領域にアクセスすることができる。但し、管理者Ｃは、サービスキー＃０００８ｈや＃１０２２Ｃｈを知らないから、基本的に、サービス定義領域＃０００８ｈや＃１０２２Ｃｈで管理されているサービス領域にアクセスすることはできない。

【０２１６】

以上のように、上位の階層のエリアキーを知らなくても、管理者は、自身のサービス領域にアクセスすることができる。

【０２１７】

ところで、上述のように、各管理者は、サービスキーを知らないサービス定義領域によって管理されるサービス領域にはアクセスすることができないが、例えば、管理者Ｃが、自身のサービス定義領域＃０３０Ｃｈによって管理されるサービス領域を利用したサービスの他、管理者Ｂ２のサービス定義領域＃１０２２ｈによって管理されるサービス領域を利用したサービスも行いたい場合がある。

【０２１８】

この場合、管理者Ｃが、サービス定義領域＃１０２２ｈによって管理されるサ

ービス領域にアクセスするには、図１４および図１５で説明したように、エリア中間キーK_{B2}、エリアコード＃０００００ｈ、＃１０００ｈ、サービスキー＃１０２２ｈ、並びにサービスコード＃１０２２ｈを知る必要があり、従って、単純には、これらの情報を、管理者Ｂ２から教えてもらう必要がある。

【０２１９】

しかしながら、管理者Ｂ２が知っているサービスキー＃１０２２ｈは、その親である管理者Ａでも知り得ないものであり、このような管理者Ｂ２しか知り得ないサービスキー＃１０２２ｈを、管理者Ｃに教えてしまうのは、セキュリティの観点から好ましくない。

【０２２０】

また、この場合、セキュリティの問題を無視しても、管理者Ｃが、サービス定義領域＃０３０Ｃｈまたは＃１０２２ｈによってそれぞれ管理される２つのサービス領域の両方にアクセスするには、ＩＣカード２において、図１５で説明した処理を行うことにより、第１アクセスキーK_{bc}および第２アクセスキーK_{ac}を生成し、サービス定義領域＃０３０Ｃｈによって管理されるサービス領域へのアクセスのための相互認証を行うとともに、図１７で説明した処理を行うことにより第１アクセスキーK_{bc}および第２アクセスキーK_{ac}を生成し、サービス定義領域＃１０２２ｈによって管理されるサービス領域へのアクセスのための相互認証を行う必要がある。

【０２２１】

従って、サービス領域ごとに、そのサービス領域へのアクセスのための相互認証を行う場合には、各サービス領域に、迅速にアクセスすることが困難となり、その結果、例えば、図１のカードシステムを駅の改札に通用した場合には、通勤者が、改札口に設けられているゲートを通過する、比較的に短い時間に、ＩＣカード２の所定のサービス領域にアクセスして、データを書き込み、または読み出すことが困難となる。

【０２２２】

そこで、例えば、管理者Ｃが、自身のサービス定義領域＃０３０Ｃｈによって管理されるサービス領域を利用したサービスの他、管理者Ｂ２のサービス定義領

域＃１０２２ｈによって管理されるサービス領域を利用したサービスも行う場合には、セキュリティの問題を解決し、かつサービス領域への迅速なアクセスを確保するために、管理者ＣおよびＢ２との間で、例えば、図１８に示すような、情報のやりとりを行い、サービス提供装置１１１への登録を行う。

【０２２３】

即ち、管理者Ｃは、図１６における場合と同様に、サービス定義領域＃０３０Ｃｈに記憶させたサービスキー＃０３０Ｃｈを、エリア中間キーK_Cで暗号化し、サービス中間キー$K_{\#030Ch}$を生成する。さらに、管理者Ｃは、このサービス中間キー$K_{\#030Ch}$を、管理者Ｂ２に渡し、サービスキー＃１０２２ｈで暗号化してもらう。そして、管理者Ｃは、サービス中間キー$K_{\#030Ch}$の、サービスキー＃１０２２ｈでの暗号化結果であるサービス中間キー$K_{\#1022h'}$を、サービスコード＃１０２２ｈとともに受け取る。

【０２２４】

従って、管理者ＣとＢ２との間でやりとりされるキーは、サービス中間キー$K_{\#030Ch}$および$K_{\#1022h'}$だけであり、管理者Ｃしか知り得ないサービスキー＃０３０Ｃｈが、管理者Ｂ２に知られたり、また、管理者Ｂ２しか知り得ないサービスキー＃１０２２ｈが、管理者Ｃに知られることはない。即ち、セキュリティ上の問題はない。

【０２２５】

管理者Ｂ２から、サービス中間キー$K_{\#1022h'}$およびサービスコード＃１０２２ｈを受け取った管理者Ｃは、それらとともに、自身のエリア定義領域＃０３００ｈの階層より上位の階層のエリア定義領域のエリアコード、即ち、いまの場合、管理者Ａのエリア定義領域＃００００ｈのエリアコード＃００００ｈおよび管理者Ｂ１のエリア定義領域＃０１００ｈのエリアコード０１００ｈ、並びに自身のエリア定義領域＃０３００ｈのエリアコード＃０３００ｈを、サービス提供装置１１１に登録する。さらに、管理者Ｃは、エリア中間キーK_C、およびエリア定義領域＃０３００ｈの階層に作成されたサービス定義領域＃０３０Ｃｈのサービスコード＃０３０Ｃｈも、サービス提供装置１１１に登録する。

【０２２６】

この場合、サービス提供装置１１１に、ＩＣカード２が装着されると、サービス提供装置１１１とＩＣカード２との間で、次のようにして相互認証が行われる。

【０２２７】

即ち、サービス提供装置１１１は、図１９に示すように、登録されているエリアコード＃０００００ｈ、＃０１００ｈ、および＃０３００ｈと、サービスコード＃０３０Ｃｈおよび＃１０２２ｈとを、ＩＣカード２に送信する。ＩＣカード２（シーケンサ９１）では、サービス提供装置１１１からのエリアコード＃０００００ｈ、＃０１００ｈ、および＃０３００ｈ、並びにサービスコード＃０３０Ｃｈおよび＃１０２２ｈが受信される。

【０２２８】

そして、ＩＣカード２では、システム定義ブロック（図４）に記憶されているシステムキーが読み出されるとともに、サービス提供装置１１１から受信したエリアコード＃０００００ｈ、＃０１００ｈ、または＃０３００ｈを有するエリア定義領域それぞれからエリアキー＃０００００ｈ、＃０１００ｈ、または＃０３００ｈが読み出され、図１７で説明した場合と同様にして、図１８のサービス提供装置１１１に登録されているエリア中間キーK_Cと同一のキーが生成される。このエリア中間キーK_Cと同一のキーは、認証に用いる第１アクセスキーK_{bc}とされる。

【０２２９】

また、ＩＣカード２では、サービス提供装置１１１から受信したサービスコード＃０３０Ｃｈまたは＃１０２２ｈを有するサービス定義領域それぞれからサービスキー＃０３０Ｃｈまたは＃１０２２ｈが読み出される。そして、まず、サービスキー＃０３０Ｃｈで、エリア中間キーK_Cが暗号化され、その結果、サービス中間キー$K_{\#030Ch}$と同一のキーが生成される。さらに、そのサービス中間キー$K_{\#030Ch}$と同一のキーが、サービスキー＃１０２２ｈで暗号化され、図１８のサービス提供装置１１１に登録されているサービス中間キー$K_{\#1022h'}$と同一のキーが生成される。このサービス中間キー$K_{\#1022h'}$と同一のキーは、認証に用い

る第２アクセスキーK_{ac}とされる。

【０２３０】

従って、いまの場合、サービス提供装置１１１には、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_Cまたはサービス中間キー$K_{\#1022h'}$が登録されており、ＩＣカード２では、第１アクセスキーK_{bc}または第２アクセスキーK_{ac}であるエリア中間キーK_Cまたはサービス中間キー$K_{\#1022h'}$が生成される。

【０２３１】

そして、ＩＣカード２およびサービス提供装置１１１の間で、図１２および図１３で説明した場合と同様にして、相互認証が行われる。

【０２３２】

その相互認証の結果、ＩＣカード２およびサービス提供装置１１１のいずれも適正なものと認められた場合、ＩＣカード２では、サービス提供装置１１１から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図１８および図１９で説明した場合においては、サービス定義領域＃０３０Ｃｈで管理されているサービス領域、およびサービス定義領域＃１０２２Ｃｈで管理されているサービス領域へのアクセスが可能となる。

【０２３３】

以上のように、システムキーを、２以上のエリアキーまたはサービスキーで暗号化することにより、その２以上のエリアキーまたはサービスキーを、２つの第１アクセスキーK_{bc}および第２アクセスキーK_{ac}に縮退（合成）し、その第１アクセスキーK_{bc}および第２アクセスキーK_{ac}を用いて、サービス提供装置１１１から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域へのアクセスを許可するための相互認証を行うようにしたので、複数のサービス定義領域へのアクセスを対象とする場合でも、短時間で、相互認証を終了することができ、これにより、サービス領域への迅速なアクセスを確保することができる。

【０２３４】

なお、図１２および図１３で説明した場合には、相互認証処理を、第１アクセスキーK_{bc}および第２アクセスキーK_{ac}の２つのキーを用いて行うようにしたが、例えば、第２アクセスキーK_{ac}だけを用いて行うようにすることも可能である。この場合、ＩＣカード２では、システムキーを、２以上のエリアキーまたはサービスキーで暗号化することにより、その２以上のエリアキーまたはサービスキーが、１の第２アクセスキーK_{ac}に縮退されることになる。

【０２３５】

また、相互認証には、図２０に示すように、第１アクセスキーK_{bc}および第２アクセスキーK_{ac}を、ＩＣカード２に固有の値である、例えば、製造ＩＤブロックに記憶された製造ＩＤなどで暗号化した暗号化結果を用いることも可能である。ここで、図２０においては、第１アクセスキーK_{bc}については、製造ＩＤとのＥＸＯＲをとられることで暗号化が行われており、第２アクセスキーK_{ac}については、ＤＥＳ方式による暗号化が行われている。なお、第２アクセスキーK_{ac}については、第１アクセスキーK_{bc}と製造ＩＤとのＥＸＯＲの結果をキーとして、ＤＥＳ方式による暗号化を行うことも可能である。

【０２３６】

このように、第１アクセスキーK_{bc}および第２アクセスキーK_{ac}を暗号化した暗号化結果を相互認証に用いる場合には、セキュリティを、より向上させることが可能となる。なお、この場合、サービス提供装置１１１において、製造ＩＤが必要となるが、これは、ＩＣカード２から送信するようにすれば良い。

【０２３７】

次に、ＥＥＰＲＯＭ６６の記憶領域が、エリア定義領域を階層とする階層構造をなしており、さらに、各エリア定義領域およびサービス定義領域が、認証のためのエリアキーおよびサービスキーを記憶するようになされている結果、例えば、次のような、フレキシビリティのあるアクセス制御を行うことができる。

【０２３８】

即ち、例えば、ある管理者を、親の管理者として、そのリソースを分け与えられた子の管理者が、不正なサービスなどを行っており、そのサービスの提供を停

止させたい場合には、親の管理者が、そのエリア定義領域に記憶されたエリアキーを変更することで、子の管理者による、ＩＣカード２へのアクセスを禁止することができる。

【０２３９】

具体的には、例えば、図５において、管理者Ｂ１が、管理者Ｃによるサービスの提供を停止させる場合、ＩＣカード２のエリア定義領域＃０１００ｈに記憶されたエリアキー＃０１００ｈを変更する。この場合、図１７において、ＩＣカード２において生成されるエリア中間キーK_{B1}、さらには、エリア中間キーK_Cも変更されることとなるから、変更前のエリア中間キーK_Cしか知らない管理者Ｃは、サービス定義領域＃０３０Ｃｈにアクセスすることはできなくなる。

【０２４０】

なお、管理者Ｃの親の管理者である管理者Ｂ１の、さらに親の管理者である管理者Ａが、そのエリア定義領域＃００００ｈに記憶されたエリアキー＃００００ｈを変更することによっても、サービス定義領域＃０３０Ｃｈへのアクセスを禁止することが可能である。但し、この場合は、管理者Ａの子の管理者Ｂ２が、自身のサービス定義領域＃１０２２ｈによって管理されるサービス領域にアクセスすることもできなくなる。即ち、ある管理者が、そのエリアキーを変更した場合には、そのエリア定義領域の階層の中にある階層（子の階層、孫の階層、・・・）のエリア定義領域が管理しているサービス定義領域へのアクセスはできなくなる。

【０２４１】

また、図１８および図１９では、管理者Ｃが、管理者Ｂ２のサービス定義領域＃１０２２ｈ（によって管理されるサービス領域）を、管理者Ｂ２と共有する場合について説明したが、キーの管理によっては、管理者どうしの間で、より複雑な関係のサービス定義領域の共有が可能となる。

【０２４２】

具体的には、例えば、いま、ＥＥＰＲＯＭ６６において、図２１に示すような階層構造が構成されているとする。即ち、図２１では、ＩＣカード２の発行者でもある管理者Ａのエリア定義領域＃００００ｈの階層の子の階層として、管理者

Ｅのエリア定義領域＃５０００ｈ、および管理者Ｇのエリア定義領域＃７０００ｈが作成されている。さらに、管理者Ｅのエリア定義領域＃５０００ｈの階層には、サービス定義領域＃５００８ｈ、＃５０４８ｈ、＃５０８８ｈ、および＃５０Ｃ８ｈが作成されているとともに、管理者Ｆのエリア定義領域＃６０００ｈが作成されている。

【０２４３】

また、管理者Ｆのエリア定義領域＃６０００ｈの階層には、サービス定義領域＃６００８ｈおよび＃６０４８ｈが作成されており、管理者Ｇのエリア定義領域＃７０００ｈの階層には、サービス定義領域＃７００８ｈおよび＃７０Ｃ８ｈが作成されている。

【０２４４】

以上のような階層構造において、管理者Ａは、図２２（Ａ）に示すように、システムキーを、エリアキー＃００００ｈで暗号化し、その暗号化結果を、子の管理者である管理者ＥおよびＧに渡す。

【０２４５】

管理者Ｅは、図２２（Ｂ）に示すように、管理者Ａからの、システムキーの、エリアキー＃００００ｈでの暗号化結果を、エリアキー＃５０００ｈで暗号化し、その暗号化結果を、第１アクセスキーK_{E1}として用いることとする。さらに、管理者Ｅは、第１アクセスキーK_{E1}（エリアキー＃５０００ｈによる暗号化結果）を、サービスキー＃５００８ｈ、＃５０４８ｈ、＃５０８８ｈ、＃５０Ｃ８ｈで順次暗号化し、その最終的な暗号化結果を、第２アクセスキーK_{E2}として用いることとする。

【０２４６】

また、管理者Ｆは、図２２（Ｃ）に示すように、管理者Ｅから第１アクセスキーK_{E1}（エリアキー＃５０００ｈによる暗号化結果）をもらい、それを、エリアキー＃６０００ｈで暗号化し、その暗号化結果を、第１アクセスキーK_{F1}とする。さらに、管理者Ｆは、第１アクセスキーK_{F1}（エリアキー＃６０００ｈによる暗号化結果）を、サービスキー＃６００８ｈ，＃６０４８ｈで順次暗号化する。そして、その暗号化結果を、管理者Ｅに渡し、サービスキー＃５０４８ｈ、＃５

０８８ｈで順次暗号化してもらう。その後、管理者Ｆは、その暗号化結果を、管理者Ｅからもらい、管理者Ｇに渡し、サービスキー＃７０Ｃ８ｈで暗号化してもらう。そして、管理者Ｆは、その暗号化結果を、管理者Ｇからもらい、第２アクセスキーK_{F2}として用いることとする。

【０２４７】

一方、管理者Ｇは、図２２（Ｄ）に示すように、管理者Ａからの、システムキーの、エリアキー＃００００ｈでの暗号化結果を、エリアキー＃７０００ｈで暗号化し、その暗号化結果を、第１アクセスキーK_{G1}として用いることとする。さらに、管理者Ｇは、第１アクセスキーK_{G1}（エリアキー＃７０００ｈによる暗号化結果）を、サービスキー＃７００８ｈ、＃７０Ｃ８ｈで順次暗号化し、その最終的な暗号化結果を、管理者Ｆに渡して、サービスキー＃６０４８ｈで暗号化してもらう。その後、管理者Ｇは、管理者Ｆによるサービスキー＃６０４８を用いた暗号化結果を、管理者Ｅに渡し、サービスキー＃５０８８ｈ、＃５０Ｃ８ｈで順次暗号化してもらう。そして、管理者Ｇは、その暗号化結果を、管理者Ｅからもらい、第２アクセスキーK_{G2}として用いることとする。

【０２４８】

この場合、ＩＣカード２において、図２２で説明した場合と同様の手順で、ＥＥＰＲＯＭ６６に記憶されているエリアキー、サービスキーを用いて、システムキーを暗号化し、第１アクセスキーおよび第２アクセスキーを生成することで、管理者Ｅ，Ｆ，Ｇ相互の間では、図２３に示すようなサービス定義領域の共有が可能となる。

【０２４９】

即ち、管理者Ｅは、自身のサービス定義領域＃５００８、＃５０４８ｈ、＃５０８８ｈ、＃５０Ｃ８ｈのみにアクセスすることができる。管理者Ｆは、自身のサービス定義領域＃６００８ｈ、＃６０４８ｈにアクセスする他、管理者Ｅのサービス定義領域＃５０４８ｈ、＃５０８８ｈ、および管理者Ｇのサービス定義領域＃７０Ｃ８ｈにアクセスすることが可能となる。管理者Ｇは、自身のサービス定義領域＃７００８ｈ、＃７０Ｃ８ｈにアクセスする他、管理者Ｅのサービス定義領域＃５０８８ｈ、＃５０Ｃ８ｈ、および管理者Ｆのサービス定義領域＃６０

４８ｈにアクセスすることが可能となる。

【０２５０】

なお、図２２に示したようなキーの受け渡しにおいて、ある管理者のサービスキー自体が、他の管理者に知られることはない。即ち、管理者Ｅのサービスキー＃５００８ｈ、＃５０４８ｈ、＃５０８８ｈ、＃５０Ｃ８ｈは、親の管理者Ａは勿論、管理者ＦおよびＧにも知られることはない。同様に、管理者Ｆのサービスキー＃６００８ｈ、＃６０４８ｈは、管理者ＥおよびＧに知られることはなく、管理者Ｇのサービスキー＃７００８ｈ、＃７０Ｃ８ｈは、管理者ＥおよびＦに知られることはない。

【０２５１】

また、上述したように、ある管理者が、そのエリアキーを変更した場合には、そのエリア定義領域の階層の中にある階層のエリア定義領域が管理しているサービス定義領域すべてへのアクセスはできなくなるが、即ち、親の管理者がエリアキーを変更した場合には、その子の管理者は、ＩＣカード２へのアクセスをすることができなくなるが、キー管理の仕方によっては、特定の子の管理者だけのアクセスを禁止することが可能となる。

【０２５２】

具体的には、例えば、いま、ＥＥＰＲＯＭ６６において、図２４に示すような階層構造が構成されているとする。即ち、図２４では、ＩＣカード２の発行者でもある管理者Ａのエリア定義領域＃０００００ｈの階層の子の階層として、管理者Ｈのエリア定義領域＃８０００ｈ、管理者Ｉのエリア定義領域＃９０００ｈ、および管理者Ｊのエリア定義領域＃Ａ０００ｈが作成されている。さらに、管理者Ｈのエリア定義領域＃８０００ｈの階層には、サービス定義領域＃８００８ｈ、＃８１０４ｈ、および＃８１０５ｈが作成されている。

【０２５３】

以上のような階層構造において、管理者Ａは、図２５（Ａ）に示すように、システムキーを、エリアキー＃００００ｈで暗号化し、その暗号化結果を、子の管理者である管理者ＩおよびＪに渡す。

【０２５４】

管理者Ｉは、図２５（Ｃ）に示すように、管理者Ａからの、システムキーの、エリアキー＃０００００ｈでの暗号化結果を、エリアキー＃９０００ｈで暗号化し、その暗号化結果を、第１アクセスキーK_{I1}として用いることとする。さらに、管理者Ｉは、第１アクセスキーK_{I1}（エリアキー＃９０００ｈによる暗号化結果）を、管理者Ｈに渡し、図２５（Ｂ）に示すように、サービスキー＃８００８ｈ、＃８１０４ｈで順次暗号化してもらう。そして、管理者Ｉは、その暗号化結果を、図２５（Ｃ）に示すように、第２アクセスキーK_{I2}として用いることとする。

【０２５５】

また、管理者Ｊは、図２５（Ｄ）に示すように、管理者Ａからの、システムキーの、エリアキー＃００００ｈでの暗号化結果を、エリアキー＃Ａ０００ｈで暗号化し、その暗号化結果を、第１アクセスキーK_{J1}として用いることとする。さらに、管理者Ｊは、第１アクセスキーK_{J1}（エリアキー＃Ａ０００ｈによる暗号化結果）を、管理者Ｈに渡し、図２５（Ｂ）に示すように、サービスキー＃８００８ｈ、＃８１０５ｈで順次暗号化してもらう。そして、管理者Ｊは、その暗号化結果を、図２５（Ｄ）に示すように、第２アクセスキーK_{J2}として用いることとする。

【０２５６】

この場合、ＩＣカード２において、図２５で説明した場合と同様の手順で、ＥＥＰＲＯＭ６６に記憶されているエリアキー、サービスキーを用いて、システムキーを暗号化し、第１アクセスキーおよび第２アクセスキーを生成することで、管理者Ｉは、管理者Ｈのサービス定義領域＃８００８ｈおよび＃８１０４ｈにアクセスすることが、管理者Ｊは、管理者Ｈのサービス定義領域＃８００８ｈおよび＃８１０５ｈにアクセスすることが、それぞれ可能となる。

【０２５７】

一方、管理者Ｈは、サービス定義領域＃８００８ｈを、管理者ＩおよびＪとの間でデータを共有するものとして作成しておき、サービス定義領域＃８１０４ｈまたは＃８１０５ｈを、管理者ＩまたはＪそれぞれによるサービス定義領域＃８

００８ｈへのアクセスを制御するための、いわばダミーのサービス定義領域として作成しておく。従って、サービス定義領域＃８１０４ｈおよび＃８１０５ｈで管理されるサービス領域は必要なく、その容量は０ブロックで良い。

【０２５８】

この場合において、管理者Ｈが、例えば、サービスキー＃８１０４ｈを変更すると、ＩＣカード２において、そのサービスキー＃８１０４ｈを用いて、第２アクセスキーK_{I2}が生成されて認証が行われる管理者Ｉは、サービス定義領域＃８００８ｈにアクセスすることができなくなる。即ち、管理者Ｉによるサービス定義領域＃８００８ｈへのアクセスだけが禁止される。一方、管理者Ｈが、例えば、サービスキー＃８１０５ｈを変更すると、ＩＣカード２において、そのサービスキー＃８１０５ｈを用いて、第２アクセスキーK_{J2}が生成されて認証が行われる管理者Ｊは、サービス定義領域＃８００８ｈにアクセスすることができなくなる。即ち、管理者Ｊによるサービス定義領域＃８００８ｈへのアクセスだけが禁止される。

【０２５９】

以上のように、ダミーのサービス定義領域を利用することで、特定の子の管理者だけのアクセスを禁止することができる。

【０２６０】

次に、図６で説明したように、管理者が、エリア定義領域やサービス定義領域を作成するのに必要な、コード範囲や、割り当てブロック数、エリアキー、サービスキーなどの、ユーザブロックを管理するための管理情報（以下、適宜、発券情報ともいう）を、発券機１０１に登録し、発券作業が行われる場合において、発券機１０１が、例えば、駅や、小売店、その他の安全でない場所に設置されているときには、前述したように、盗聴や改竄等の不正行為が行われる蓋然性の高く、セキュリティ管理上好ましくない。

【０２６１】

そこで、ここでは、図２６に示すように、エリア定義領域やサービス定義領域を作成しようとする管理者（以下、適宜、発券業者という）が、発券情報を暗号化し、その暗号化された発券情報を、例えば、公衆回線やインターネット、地上

波、衛星回線、ＣＡＴＶ（Cable Television）網などの伝送媒体１２１を介して、発券機１０１に伝送して登録するようにしている。そして、発券機１０１では、ＩＣカード２に、暗号化された発券情報が送信され、さらに、ＩＣカード２では、その暗号化された発券情報が復号され、エリア定義領域やサービス定義領域の作成が行われるようになされている。

【０２６２】

ここで、図２６は、管理者＃１がサービスを提供するための記憶領域だけが構成されていたＩＣカード２に、上述のようにして、管理者＃２がサービスを提供するための記憶領域が構成された状態（発券作業が行われた状態）を示している。

【０２６３】

次に、図２７は、以上のような発券作業を行う発券処理システムの一実施の形態の構成例を示している。

【０２６４】

発券情報提供装置１３１は、後述する発券情報提供処理を行うことで、暗号化された発券情報（以下、適宜、暗号化発券情報という）を、伝送媒体１２１を介して、発券機１０１に送信する。発券機１０１は、発券情報提供装置１３１からの暗号化発券情報を受信して登録する。そして、発券機１０１は、ＩＣカード２が装着されると、暗号化発券情報を、ＩＣカード２に送信する。ＩＣカード２は、発券機１０１から暗号化発券情報を受信し、後述する復号処理を行うことで、暗号化発券情報を、元の発券情報に復号する。そして、ＩＣカード２は、上述のエリア作成処理（図７）またはサービス作成処理（図８）を行うことで、復号した発券情報に基づき、エリア定義領域またはサービス定義領域をそれぞれ作成する。

【０２６５】

次に、図２８のフローチャートを参照して、発券情報提供装置１３１が行う発券情報提供処理について説明する。

【０２６６】

発券情報提供装置１３１には、エリア定義領域を作成するのに必要な、例えば

、コード範囲、割り当てブロック数、エリアキー、またはサービス定義領域を作成するのに必要な、例えば、サービスコード、割り当てブロック数、サービスキーが入力される。そして、ステップＳ２１において、これらの入力情報に基づいて、発券情報が作成される。

【０２６７】

即ち、エリア定義領域を作成するのに必要なコード範囲、割り当てブロック数、エリアキーが入力された場合には、それらを対応付けることで、発券情報が作成される。また、サービス定義領域を作成するのに必要なサービスコード、割り当てブロック数、サービスキーが入力された場合には、それらを対応付けることで、発券情報が作成される。

【０２６８】

そして、ステップＳ２２に進み、ステップＳ２１で作成された発券情報について、例えば、誤り訂正符号が演算され、これが、改竄をチェックするためのチェックコードとして、発券情報に含められる。

【０２６９】

その後、ステップＳ２３において、発券情報が暗号化される。即ち、ステップＳ２３では、例えば、発券情報によって作成しようとしているエリア定義領域またはサービス定義領域の親の階層のエリア定義領域のエリアキーで、その発券情報が暗号化され、暗号化発券情報とされる。

【０２７０】

そして、ステップＳ２４に進み、暗号化発券情報に対し、そのヘッダとして、識別コード（暗号化発券情報が、エリア定義領域を作成するためのものである場合には、そのエリアコードであり、サービス定義領域を作成するためのものである場合には、そのサービスコード）が付加され、伝送媒体１２１を介して、発券機１０１に送信されて、発券情報提供処理を終了する。

【０２７１】

従って、例えば、図５において、親の管理者Ａが、子の管理者Ｂ１のエリア定義領域＃０１００ｈを作成する場合には、図２９（Ａ）に示すような暗号化発券情報が、発券情報提供装置１３１から送信される。即ち、図２９（Ａ）の暗号化

発券情報の先頭には、ヘッダとして、エリア定義領域＃０１００ｈのエリアコード＃０１００ｈが配置されている。なお、このエリアコード＃０１００ｈは、ＩＣカード２において、親の階層を認識するために、暗号化されていない。また、発券情報提供装置１３１において、エリアコード＃０１００ｈは、入力情報のうちのコード範囲から認識される。これは、上述したように、本実施の形態では、エリア定義領域については、そのコード範囲の最小値が、エリアコードとされるため、エリアコードは、コード範囲から認識することができるからである。

【０２７２】

暗号化されていない、ヘッダとしてのエリアコード＃０１００ｈの後には、エリア定義領域＃０１００ｈに記憶させるべきコード範囲＃０１００ｈ－＃０３ＦＦｈ、割り当てブロック数３３、エリアキー＃０１００ｈとしてのa0a0a0a0a0a0a0a0、チェックコードが順次配置されている。そして、これらは、親の階層であるエリア定義領域＃００００ｈのエリアキー＃００００ｈとしての0123456789abcdefで暗号化（図２９（Ａ）において影を付して示す）されている。

【０２７３】

また、例えば、図５において、管理者Ｂ２が、自身のサービス定義領域＃１０２２ｈを作成する場合には、図２９（Ｂ）に示すような暗号化発券情報が、発券情報提供装置１３１から送信される。即ち、図２９（Ｂ）の暗号化発券情報の先頭には、ヘッダとして、サービス定義領域＃１０２２ｈのサービスコード＃１０２２ｈが配置されている。なお、このサービスコード＃１０２２ｈは、ＩＣカード２において、親の階層（サービス定義領域が属する階層）を認識するために、暗号化されていない。

【０２７４】

暗号化されていない、ヘッダとしてのサービスコード＃１０２２ｈの後には、サービス定義領域＃１０２２ｈに記憶させるべきサービスコード＃１０２２ｈ、割り当てブロック数５、エリアキー＃１０２２ｈとしての0303030303030303、チェックコードが順次配置されている。そして、これらは、親の階層であるエリア定義領域＃１０００ｈのエリアキー＃１０００ｈとしてのc0c0c0c0c0c0c0c0で暗号化（図２９（Ｂ）において影を付して示す）されている。

【０２７５】

以上のように、発券情報は、親の階層のエリアキーで暗号化されるため、そのエリアキーを知らない限り、発券情報の内容も知ることができない。従って、そのような暗号化発券情報を、安全でない場所に送信しても、その内容の漏洩を防止することができる。さらに、その結果、例えば、暗号化発券情報を、第三者に配布して、発券機１０１への登録や、ＩＣカード２への送信などを依頼することが可能となる。

【０２７６】

なお、ここでは、発券情報を、親の階層のエリアキーで暗号化することとしているため、発券情報提供処理は、基本的に、その親の管理者の下で行うのが望ましい。即ち、第三者に、発券情報提供処理を行わせる場合には、暗号化に用いる親の階層のエリアキーを、その第三者に公開しなければならず、セキュリティ上好ましくないため、発券情報提供処理は、親の管理者の下で行うのが望ましい。

【０２７７】

次に、図３０のフローチャートを参照して、ＩＣカード２が行う復号処理について説明する。

【０２７８】

上述したように、発券機１０１は、発券情報提供装置１３１から、暗号化発券情報が送信されてくると、それを受信して登録する。そして、発券機１０１は、ＩＣカード２が装着されると、暗号化発券情報を、ＩＣカード２に送信する。ＩＣカード２は、発券機１０１から暗号化発券情報を受信し、ステップＳ３１において、その暗号化発券情報によって作成するエリア定義領域またはサービス定義領域の親の階層としてのエリア定義領域を認識する。

【０２７９】

即ち、ステップＳ３１では、暗号化発券情報のヘッダを参照することで、作成対象のエリア定義領域またはサービス定義領域のエリアコードまたはサービスコードが認識される。さらに、ステップＳ３１では、その認識されたエリアコードまたはサービスコードを、コード範囲に含むエリア定義領域が、ＥＥＰＲＯＭ６６から検出され、そのエリア定義領域が、親の階層として認識される。

【０２８０】

そして、ステップＳ３２に進み、ステップＳ３１で認識された親の階層のエリア定義領域に記憶されているエリアキーで、暗号化発券情報が復号され、ステップＳ３３に進む。ステップＳ３３では、復号された発券情報に含まれるチェックコードに基づいて、その発券情報の改竄が行われているか否かが判定される。ステップＳ３３において、発券情報の改竄が行われていると判定された場合、ステップＳ３４に進み、発券情報の改竄が行われている旨のメッセージを、発券機１０１に送信し、また、復号された発券情報を破棄するなどのエラー処理が行われ、復号処理を終了する。この場合、復号処理は異常終了し、エリア定義領域やサービス定義領域は作成されない。

【０２８１】

一方、ステップＳ３３において、発券情報の改竄が行われていないと判定された場合、復号処理を終了する。この場合、復号処理は正常終了し、その後、復号された発券情報をＥＥＰＲＯＭ６６に記憶させる処理、即ち、エリア定義領域またはサービス定義領域を作成するエリア作成処理（図７）またはサービス作成処理（図８）が行われる。

【０２８２】

なお、発券情報が改竄されているか否かのチェックは、チェックコードによる他、暗号化発券情報のヘッダを用いて行うことも可能である。即ち、暗号化発券情報が、エリア定義領域を作成するためのものであれば、図２９（Ａ）に示したように、そのヘッダには、エリアコードが配置され、そのエリアコードは、その後に配置された、暗号化されたコード範囲の最小値に一致しているはずである。従って、ヘッダに配置されたエリアコードと、その後に配置されたコード範囲の最小値とを比較することで、暗号化発券情報の改竄の有無をチェックすることができる。また、暗号化発券情報が、サービス定義領域を作成するためのものであれば、図２９（Ｂ）に示したように、そのヘッダには、サービスコードが配置され、そのサービスコードは、その後に配置された、暗号化されたサービスコードに一致しているはずである。従って、ヘッダに配置されたサービスコードと、その後に配置されたサービスコードとを比較することで、暗号化発券情報の改竄の

有無をチェックすることができる。

【０２８３】

以上のように、発券情報提供装置１３１において、発券情報を暗号化して、暗号化発券情報とし、ＩＣカード２において、その暗号化発券情報を復号するようにしたので、発券機１０１を安全でない場所に設置し、伝送媒体１２１を介して伝送しても、盗聴や改竄等の不正行為が行われることを防止することができる。

【０２８４】

その結果、ＩＣカード２を利用して新たなサービスの提供を開始するために発券作業を行う場合に、ＩＣカード２を回収する必要がなくなり、従って、その回収に要するコストの削減を図ることができる。また、ＩＣカード２のユーザからすれば、新たなサービスの提供が開始された場合に、ＩＣカード２を回収してもらわなくても、発券機１０１が設定されている場所に、ＩＣカード２を持っていき、発券作業を行うことで、その新たなサービスの提供を受けることが、即座に可能となる。

【０２８５】

以上、本発明を、非接触で通信が行われる非接触カードシステムに適用した場合について説明したが、本発明は、接触した状態で通信が行われるカードシステムにも適用可能である。また、本発明の適用範囲は、カードシステムに限定されるものではない。

【０２８６】

なお、本実施の形態では、認証を、いわゆる秘密鍵方式で行うようにしたが、認証は、いわゆる公開鍵方式で行うようにすることも可能である。

【０２８７】

また、本実施の形態では、あるエリア定義領域の階層のサービス定義領域にアクセスするときに、そのエリア定義領域の階層から、最上位階層までのパス上にあるエリア定義領域のエリアキーを順次用いて、第１アクセスキーを生成するようにしたが、第１アクセスキーの生成方法は、これに限定されるものではない。さらに、本実施の形態では、アクセス対象のサービス定義領域のサービスキーを順次用いて、第２アクセスキーを生成するようにしたが、第２アクセスキーの生

成方法も、これに限定されるものではない。即ち、第１アクセスキーおよび第２アクセスキーは、任意の２以上のエリアキーまたはサービスキーを順次用いて生成することが可能である。

【０２８８】

さらに、本実施の形態では、ユーザブロックおよびシステムブロックのいずれも、１のメモリであるＥＥＰＲＯＭ６６に記憶させるようにしたが、ユーザブロックとシステムブロックとは、物理的に、別々のメモリに記憶させるようにすることが可能である。

【０２８９】

また、本実施の形態では、データをＥＥＰＲＯＭに記憶させるようにしたが、データは、ＥＥＰＲＯＭ以外の半導体メモリや、磁気ディスクなどに記憶させることも可能である。

【０２９０】

さらに、本実施の形態では、発券情報提供処理において、親の階層のエリア定義領域におけるエリアキーで、発券情報を暗号化するようにしたが、発券情報の暗号化に用いるキーは、そのような親の階層のエリアキーに限定されるものではない。但し、ＩＣカード２において、暗号化発券情報を復号する必要があることから、発券情報の暗号化に用いるキーは、ＩＣカード２に記憶させておく必要がある。従って、親の階層のエリアキーを、発券情報の暗号化に用いる場合には、その親の階層のエリアキーは、既に、ＩＣカード２に記憶されているから、それとは別に、発券情報の復号（暗号化）に用いるキーを、ＩＣカード２に記憶させる必要はない。

【０２９１】

また、本実施の形態では、ＥＥＰＲＯＭ６６の記憶領域を階層構造にして管理するようにしたが、本発明は、ＥＥＰＲＯＭ６６の記憶領域が階層構造で管理されていない場合にも適用可能である。

【０２９２】

さらに、本実施の形態では、暗号化発券情報を、伝送媒体１２１を介して、発券機１０１に送信して登録するようにしたが、暗号化発券情報は、例えば、磁気

ディスクや、光磁気ディスク、光ディスク、メモリカード、磁気テープなどの記録媒体（記憶媒体）に記憶させ、それを、直接、発券機１０１に持っていくことで登録することも可能である。

【０２９３】

【発明の効果】

請求項１に記載の情報処理装置および請求項５に記載の情報処理方法によれば、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報が暗号化される。従って、管理情報の内容が第三者に知られることを防止することが可能となる。

【０２９４】

請求項６に記載の情報処理装置および請求項１０に記載の情報処理方法によれば、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものが復号される。従って、管理情報の内容が第三者に知られることを防止することが可能となる。

【図面の簡単な説明】

【図１】

本発明を適用したＩＣカードを用いたカードシステムの一実施の形態の構成例を示すブロック図である。

【図２】

図１のリーダ／ライタ１の構成例を示すブロック図である。

【図３】

図１のＩＣカード２の構成例を示すブロック図である。

【図４】

図３のＥＥＰＲＯＭ６６の論理フォーマットを示す図である。

【図５】

図３のＥＥＰＲＯＭ６６のディレクトリ構造を示す図である。

【図６】

図５の階層構造が構成されていく過程を説明するための図である。

【図７】

エリア作成処理を説明するためのフローチャートである。

【図８】

サービス作成処理を説明するためのフローチャートである。

【図９】

管理者間でのキーの受け渡しを説明するための図である。

【図１０】

管理者Ａがサービスを提供するときに必要な情報を説明するための図である。

【図１１】

管理者Ａがサービスを提供するときのＩＣカード２の処理を説明するための図である。

【図１２】

サービス提供装置１１１によるＩＣカード２の認証方法を説明するための図である。

【図１３】

ＩＣカード２によるサービス提供装置１１１の認証方法を説明するための図である。

【図１４】

管理者Ｂ２がサービスを提供するときに必要な情報を説明するための図である。

【図１５】

管理者Ｂ２がサービスを提供するときのＩＣカード２の処理を説明するための図である。

【図１６】

管理者Ｃがサービスを提供するときに必要な情報を説明するための図である。

【図１７】

管理者Ｃがサービスを提供するときのＩＣカード２の処理を説明するための図である。

【図１８】

管理者Ｃがサービスを提供するときに必要な情報を説明するための図である。

【図１９】

管理者ＣがサービスをＩＣカード２の処理を説明するための図である。

【図２０】

相互認証に用いる第１アクセスキーおよび第２アクセスキーの生成方法を説明するための図である。

【図２１】

ＥＥＰＲＯＭ６６における階層構造を示す図である。

【図２２】

管理者間でのキーの受け渡しを説明するための図である。

【図２３】

管理者間でのサービス（データ）の共有を説明するための図である。

【図２４】

ＥＥＰＲＯＭ６６における階層構造を示す図である。

【図２５】

管理者間でのキーの受け渡しを説明するための図である。

【図２６】

本発明の原理を説明するための図である。

【図２７】

本発明を適用した発券処理システムの一実施の形態の構成例を示すブロック図である。

【図２８】

発券情報提供処理を説明するためのフローチャートである。

【図２９】

暗号化発券情報のフォーマットを示す図である。

【図３０】

復号処理を説明するためのフローチャートである。

【図３１】

従来のＩＣカードの流通を説明するための図である。

【図３２】

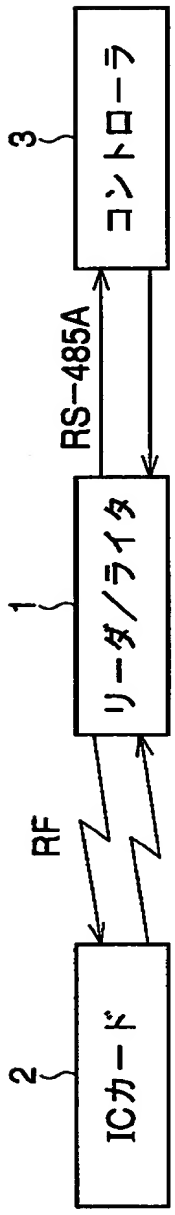
従来のＩＣカードの流通を説明するための図である。

【符号の説明】

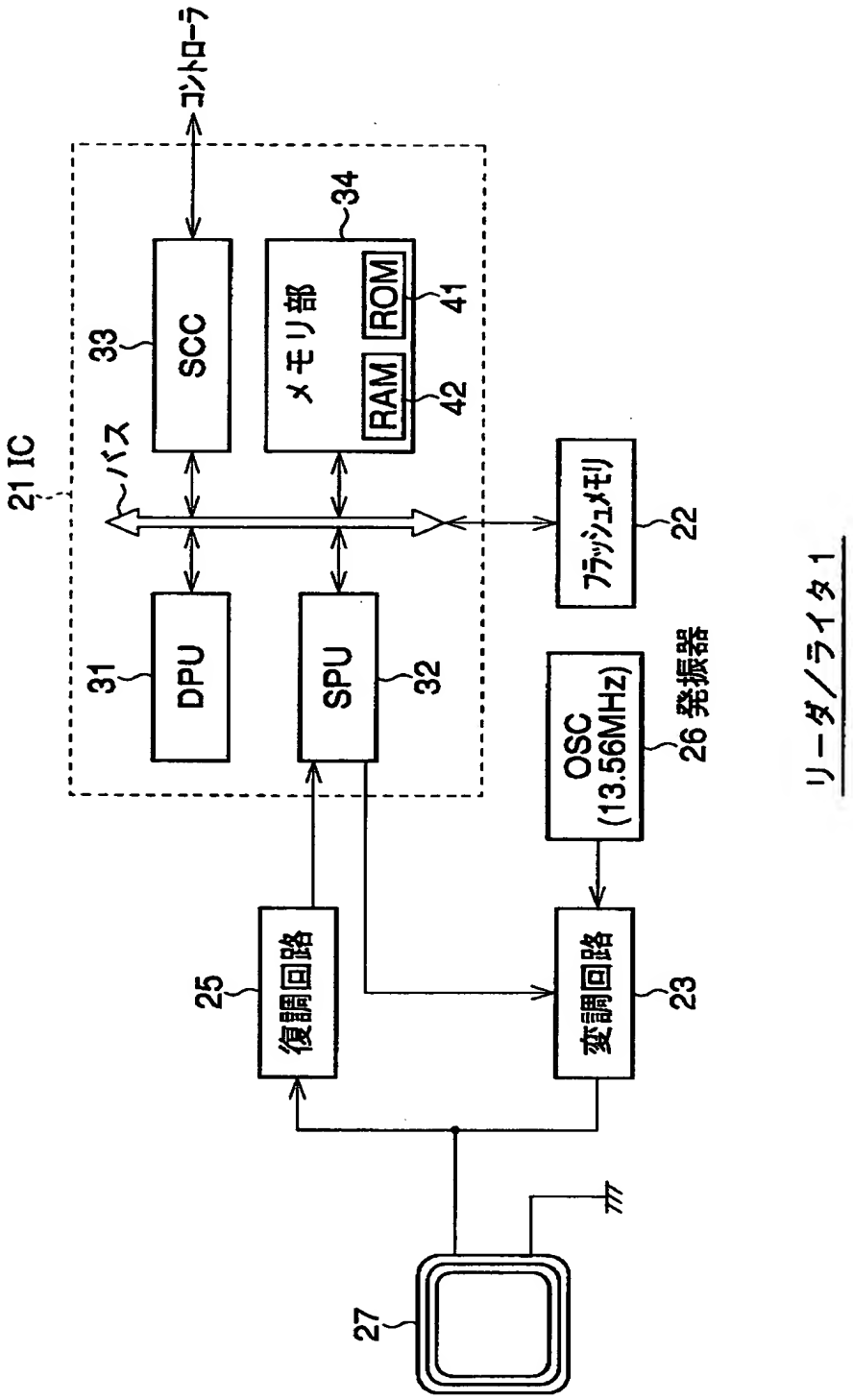
１　リーダ／ライタ，　２　ＩＣカード，　３　コントローラ，　２１　ＩＣ，　２３　変調回路，　２５　復調回路，　２７　アンテナ，　５１　ＩＣ，　５２　コンデンサ，　５３　アンテナ，　６１　ＲＦインタフェース部，　６２　ＢＰＳＫ復調回路，　６３　ＰＬＬ部，　６４　演算部，　６５　ＲＯＭ，　６６　ＥＥＰＲＯＭ，　６７　ＲＡＭ，　６８　ＢＰＳＫ変調回路，　８１　ＡＳＫ復調部，　８２　電圧レギュレータ，　８３　発振回路，　８４　ＡＳＫ変調部，　９１　シーケンサ，　９２　暗号／復号部，　９３　パリティ演算部，　１０１　発券機，　１１１　サービス提供装置，　１２１　伝送媒体，　１３１　発券情報提供装置

【書類名】図面

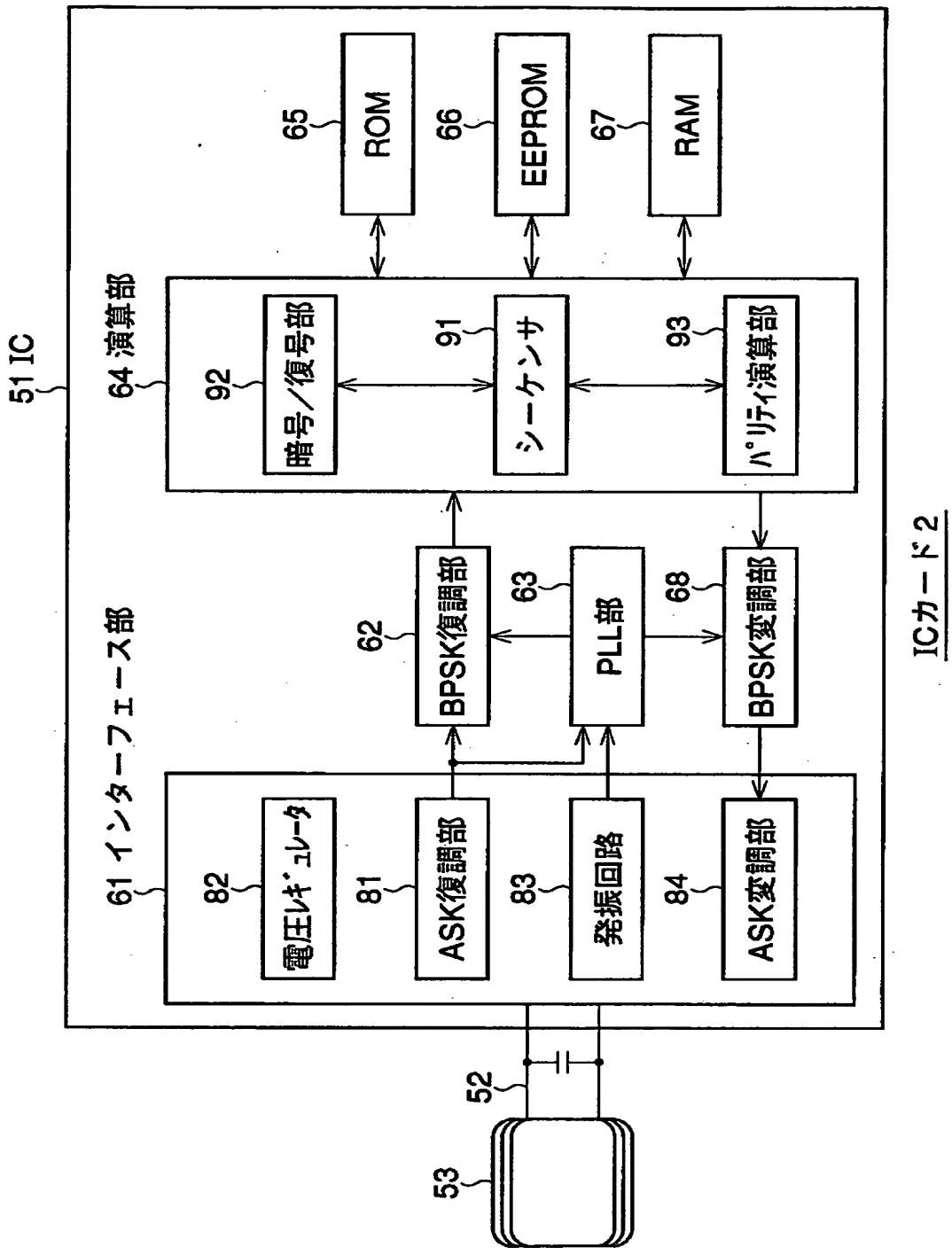
【図１】



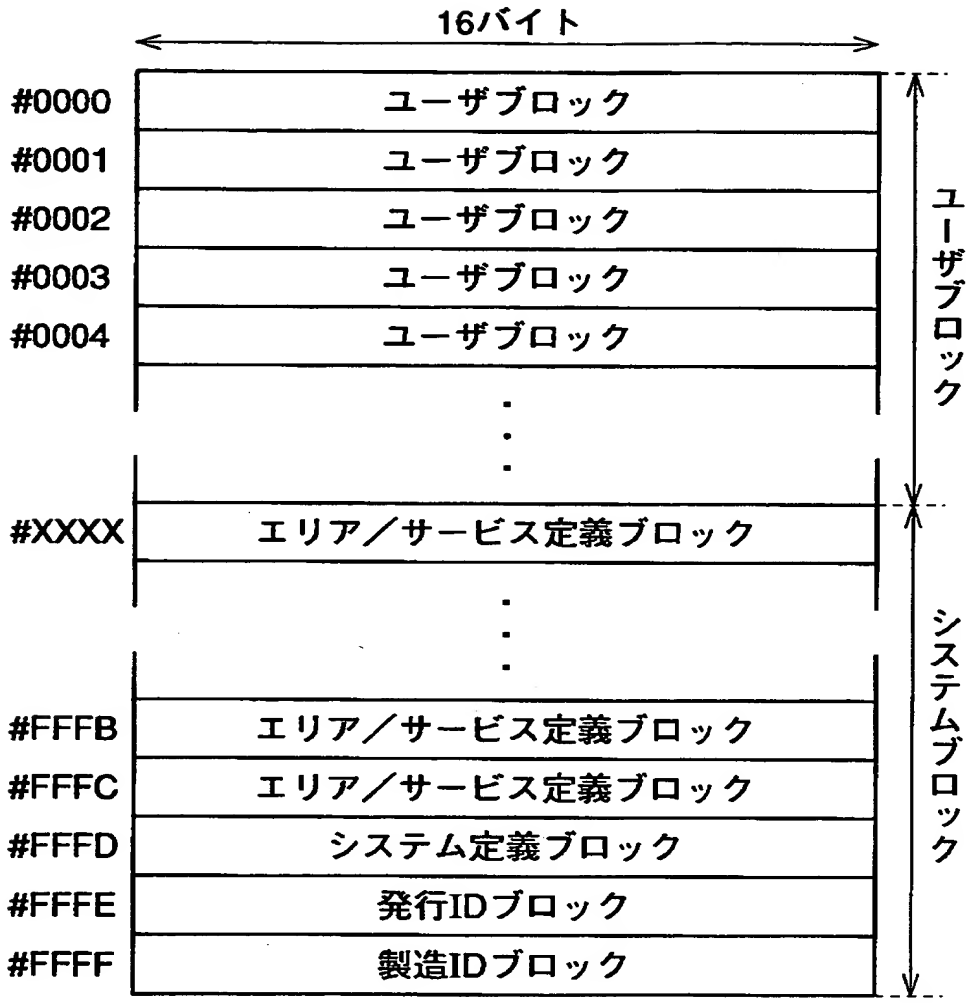
【図２】


コントローラ
34
メモリ部
ROM
41
RAM
42
33
SCC
21 IC
バス
フラッシュメモリ
22
DPU
31
SPU
32
OSC
(13.56MHz)
26 発振器
リーダ／ライタ１
25
復調回路
変調回路
23
27

【図３】

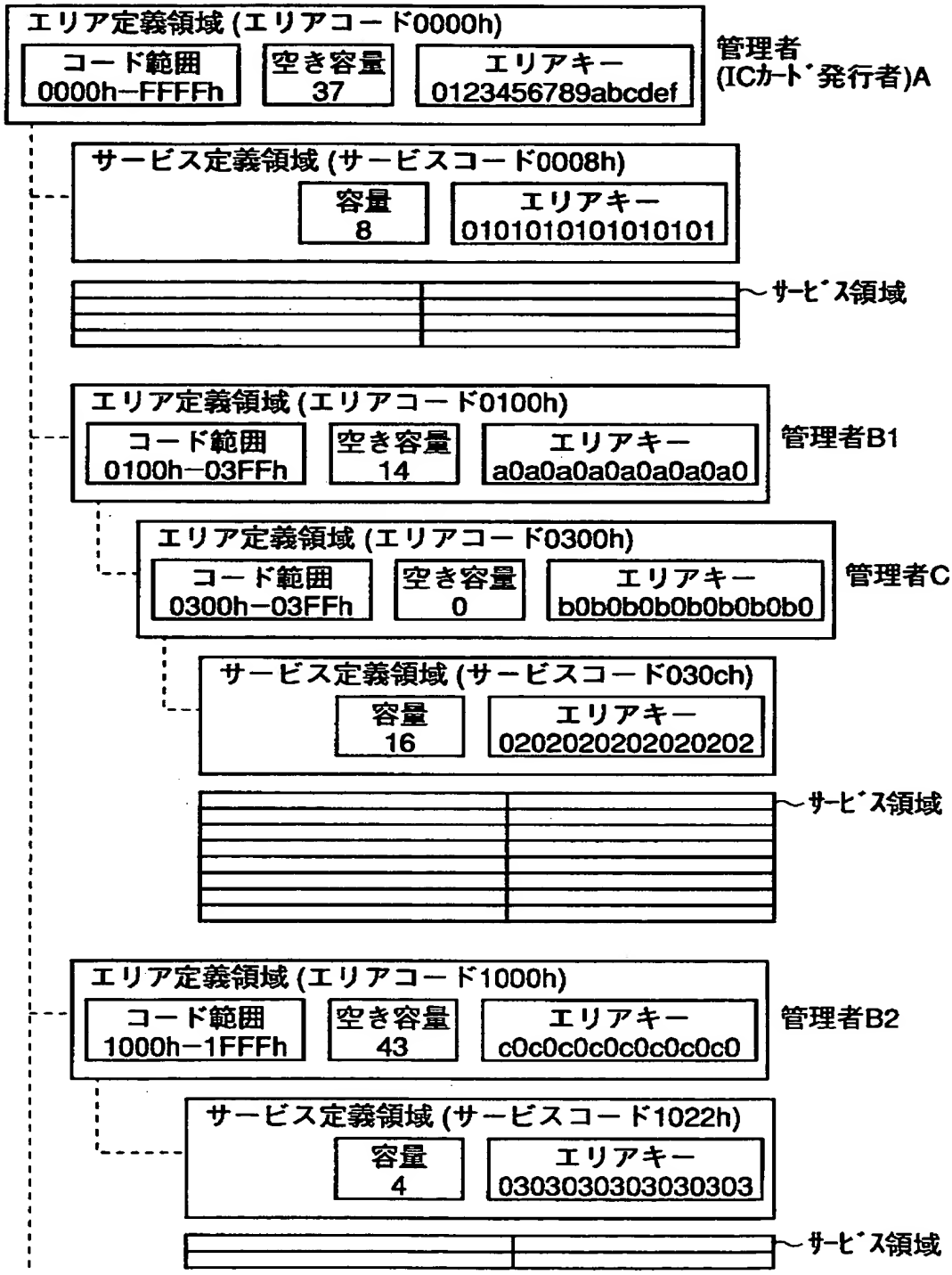

51 IC
61 インターフェース部
64 演算部
82
電圧レギュレータ
81
ASK復調部
83
発振回路
84
ASK変調部
62
BPSK復調部
63
PLL部
68
BPSK変調部
92
暗号／復号部
91
シーケンサ
93
パリティ演算部
65
ROM
66
EEPROM
67
RAM
52
53
ICカード2

【図４】



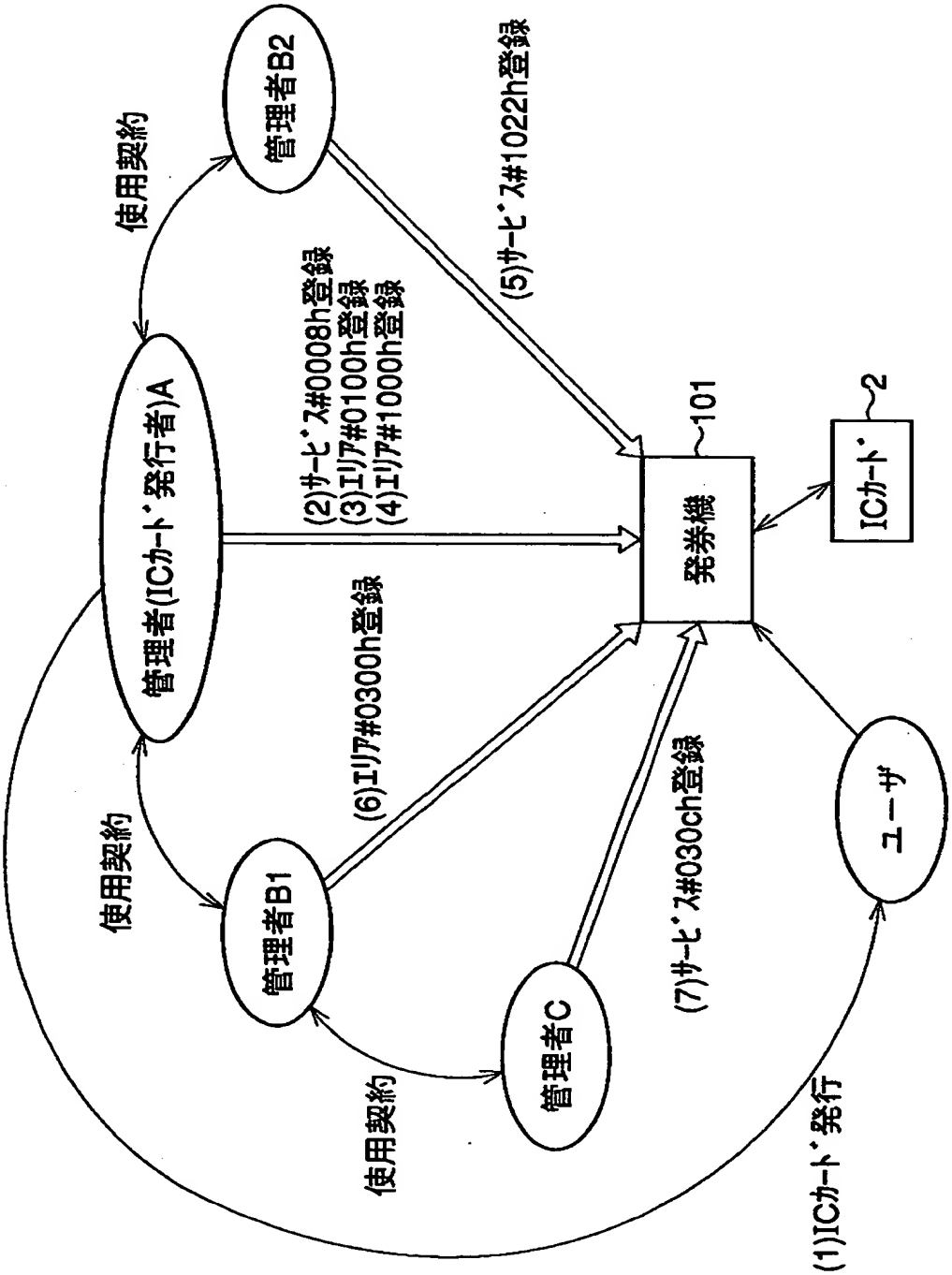
EEPROM66の論理フォーマット

【図５】

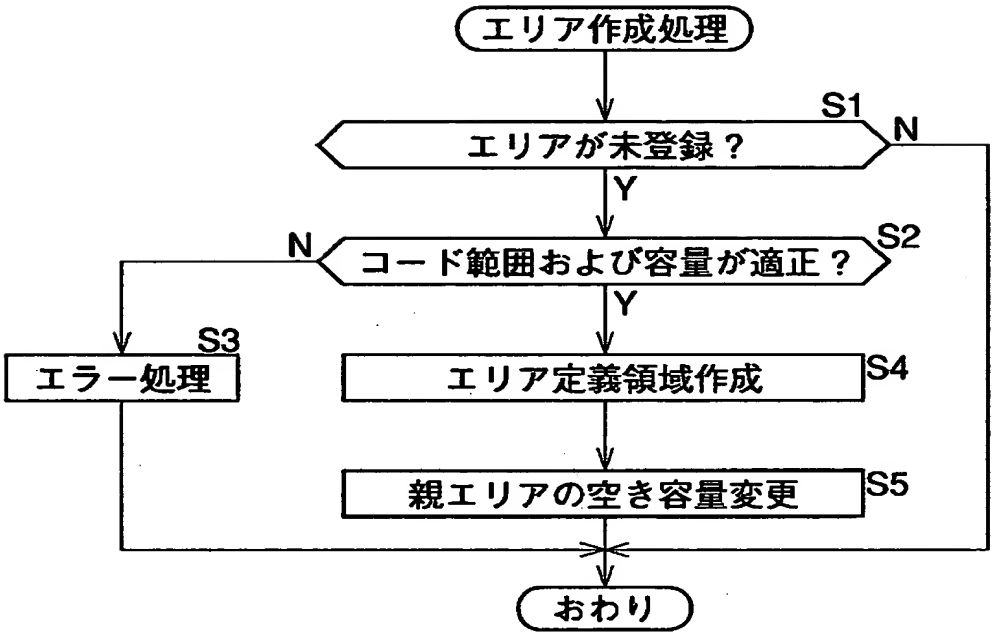

エリア定義領域 (エリアコード0000h)
コード範囲 0000h−FFFFh
空き容量 37
エリアキー 0123456789abcdef
管理者 (ICカード発行者)A
サービス定義領域 (サービスコード0008h)
容量 8
エリアキー 0101010101010101
サービス領域
エリア定義領域 (エリアコード0100h)
コード範囲 0100h−03FFh
空き容量 14
エリアキー a0a0a0a0a0a0a0a0
管理者B1
エリア定義領域 (エリアコード0300h)
コード範囲 0300h−03FFh
空き容量 0
エリアキー b0b0b0b0b0b0b0b0
管理者C
サービス定義領域 (サービスコード030ch)
容量 16
エリアキー 0202020202020202
サービス領域
エリア定義領域 (エリアコード1000h)
コード範囲 1000h−1FFFh
空き容量 43
エリアキー c0c0c0c0c0c0c0c0
管理者B2
サービス定義領域 (サービスコード1022h)
容量 4
エリアキー 0303030303030303
サービス領域

ディレクト構造

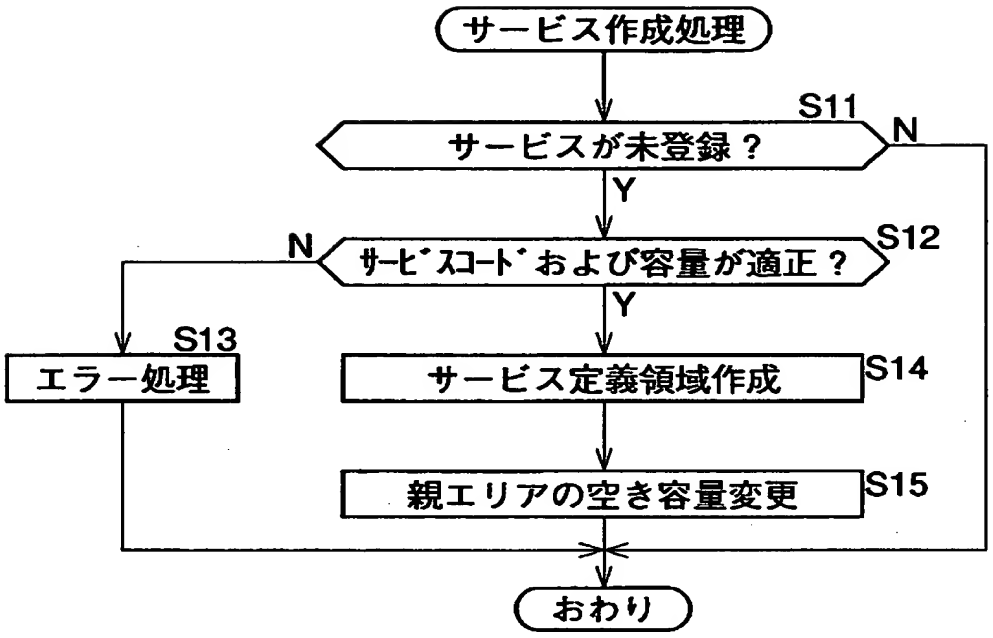
【図６】


管理者B2
使用契約
(5)ｻｰﾋﾞｽ#1022h登録
(2)ｻｰﾋﾞｽ#0008h登録
(3)ｴﾘｱ#0100h登録
(4)ｴﾘｱ#1000h登録
管理者(ICｶｰﾄﾞ発行者)A
101
発券機
2
ICｶｰﾄﾞ
使用契約
(6)ｴﾘｱ#0300h登録
管理者B1
(7)ｻｰﾋﾞｽ#030ch登録
ﾕｰｻﾞ
管理者C
使用契約
(1)ICｶｰﾄﾞ発行

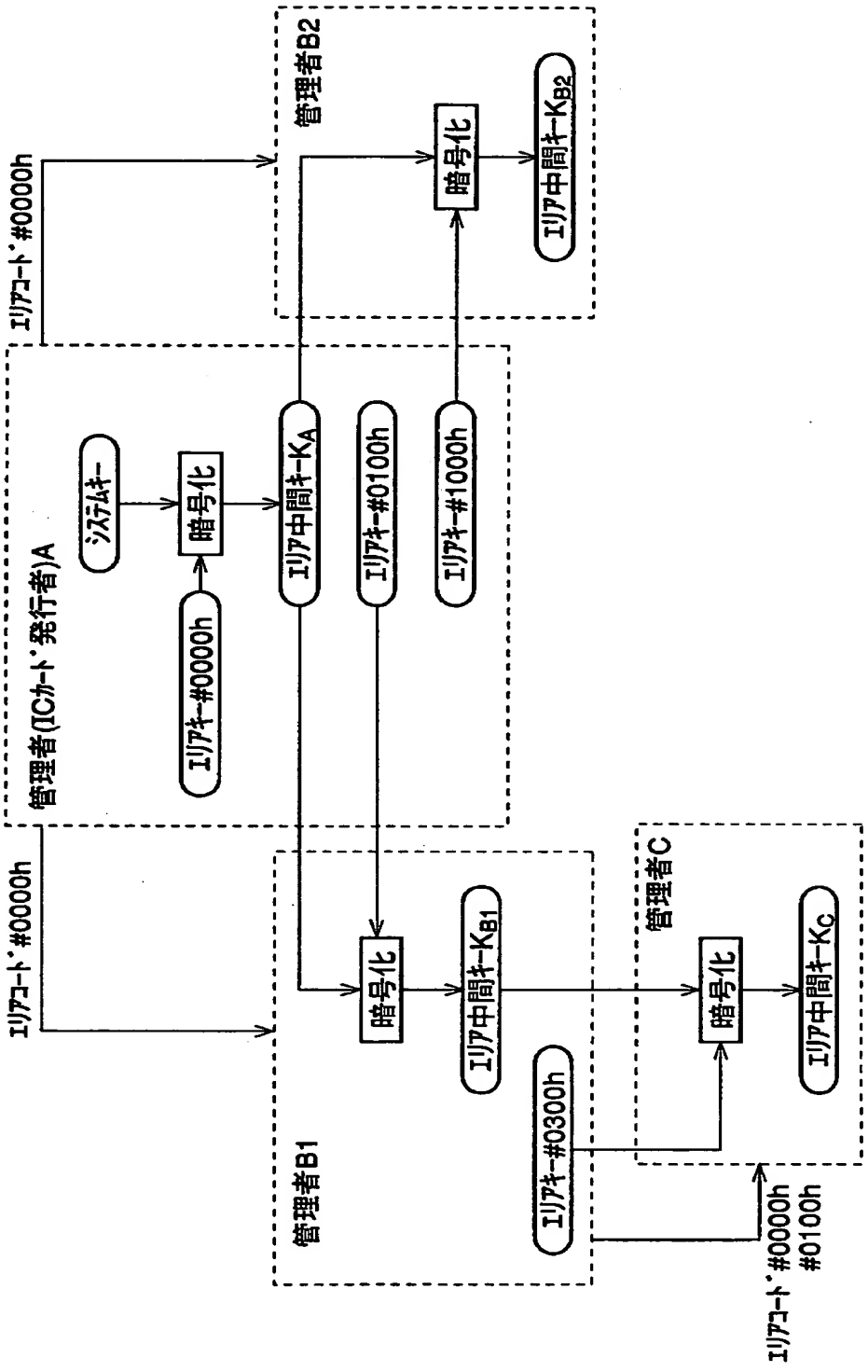
【図７】


エリア作成処理
S1
エリアが未登録？
N
Y
N
S2
コード範囲および容量が適正？
Y
S3
エラー処理
エリア定義領域作成
S4
親エリアの空き容量変更
S5
おわり

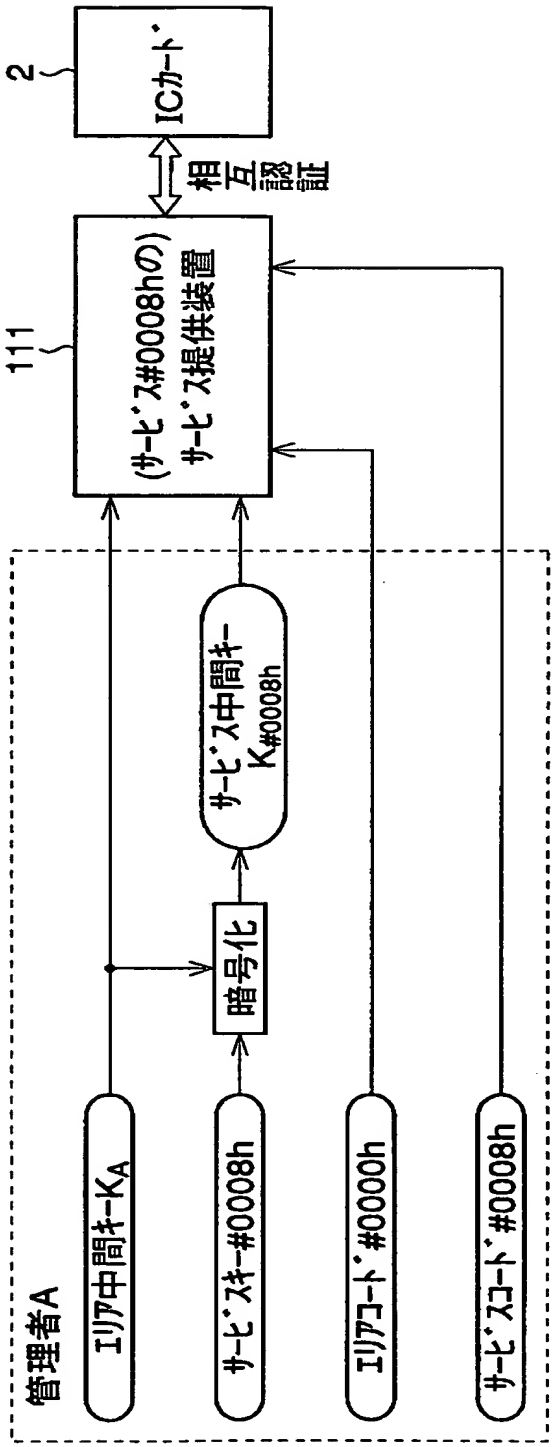
【図８】


サービス作成処理
S11
サービスが未登録？
N
Y
N
ｻｰﾋﾞｽｺｰﾄﾞおよび容量が適正？
S12
Y
S13
エラー処理
サービス定義領域作成
S14
親エリアの空き容量変更
S15
おわり

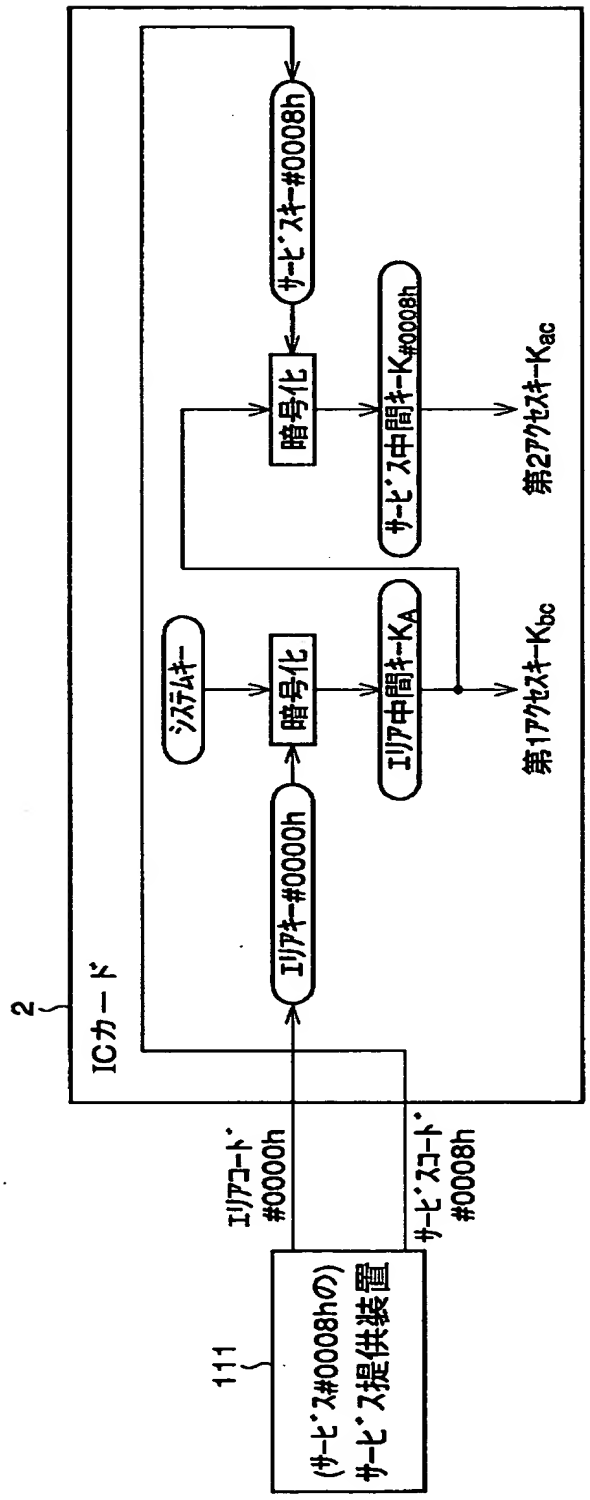
【図９】


管理者B2
暗号化
エリア中間キーK_{B2}
エリアコード'#0000h
管理者(ICカード'発行者)A
システムキー
暗号化
エリア中間キーK_A
エリアキー#0100h
エリアキー#1000h
エリアキー#0000h
エリアコード'#0000h
管理者B1
暗号化
エリア中間キーK_{B1}
エリアキー#0300h
管理者C
暗号化
エリア中間キーK_C
エリアコード'#0000h
#0100h

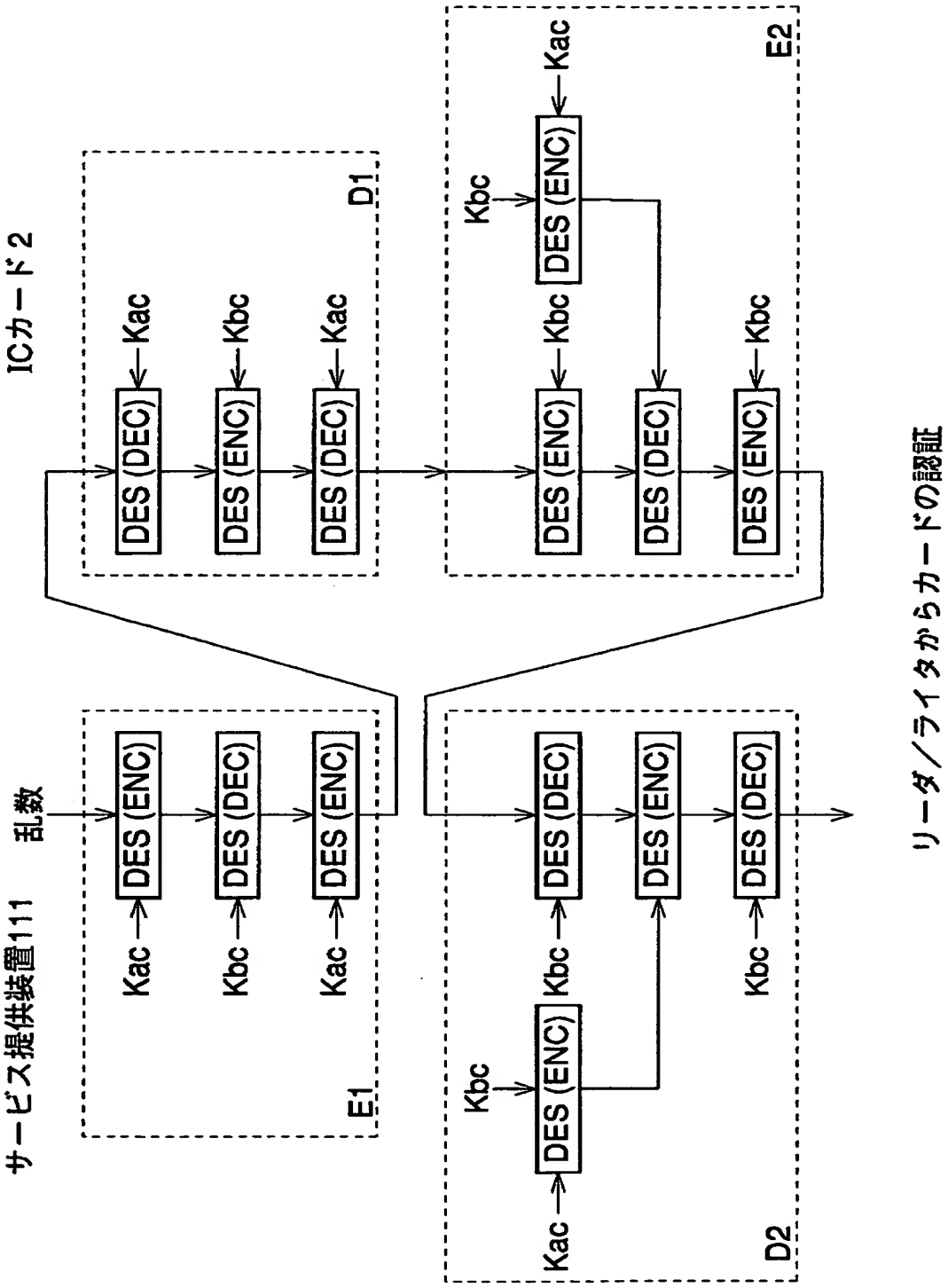
【図10】


2
ICカード
相互認証
111
(サービス#0008hの)
サービス提供装置
管理者A
エリア中間キーK_A
サービスキー#0008h
暗号化
サービス中間キー
$K_{\#0008h}$
エリアコード#0000h
サービスコード#0008h

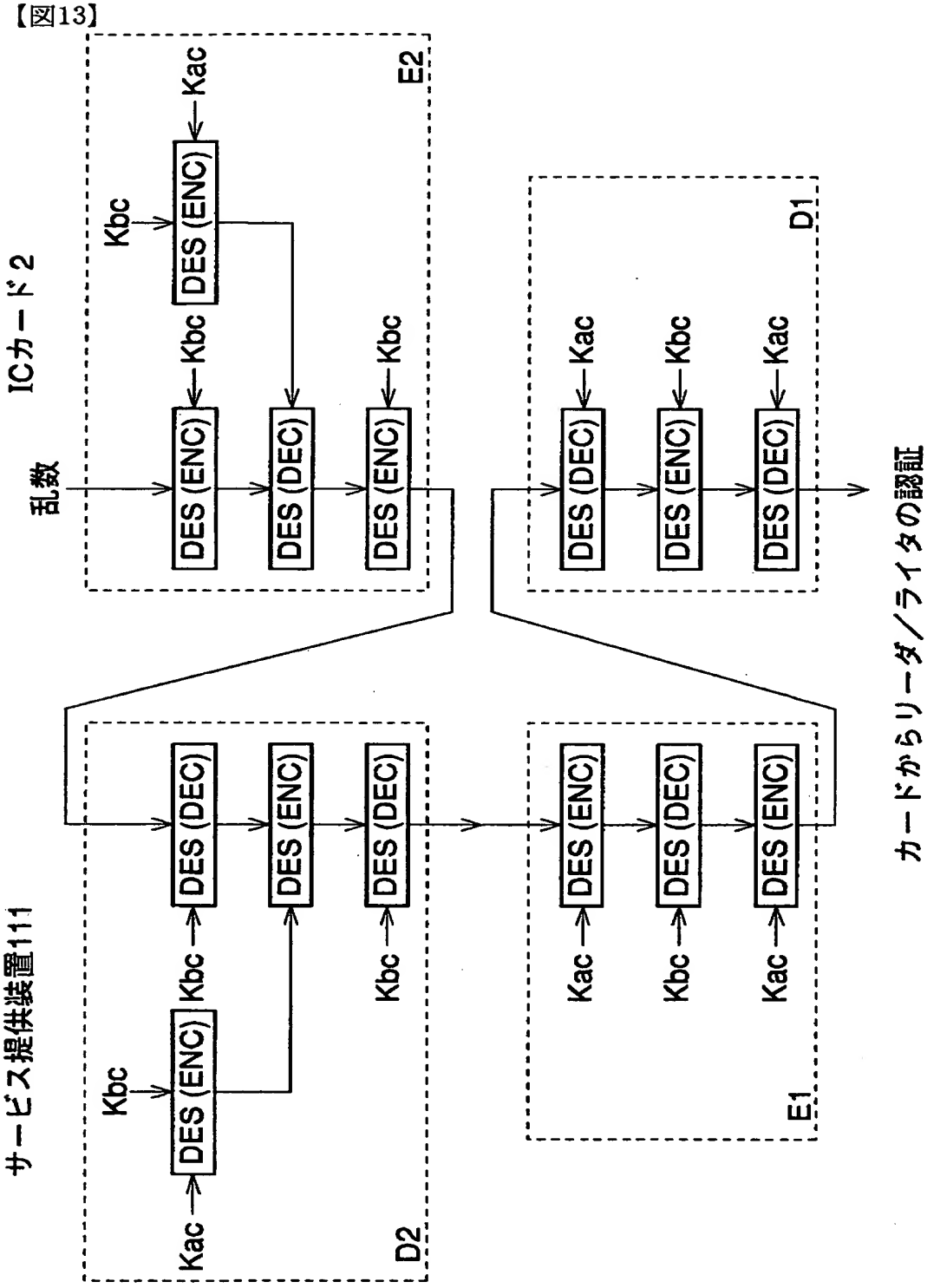
【図11】


ICカード
2
エリアキー#0000h
システムキー
暗号化
エリア中間キー-KA
第1アクセスキー-Kbc
サービス#0008hの
サービス提供装置
111
エリアコード
#0000h
サービスコード
#0008h
サービスキー#0008h
暗号化
サービス中間キー-K#0008h
第2アクセスキー-Kac

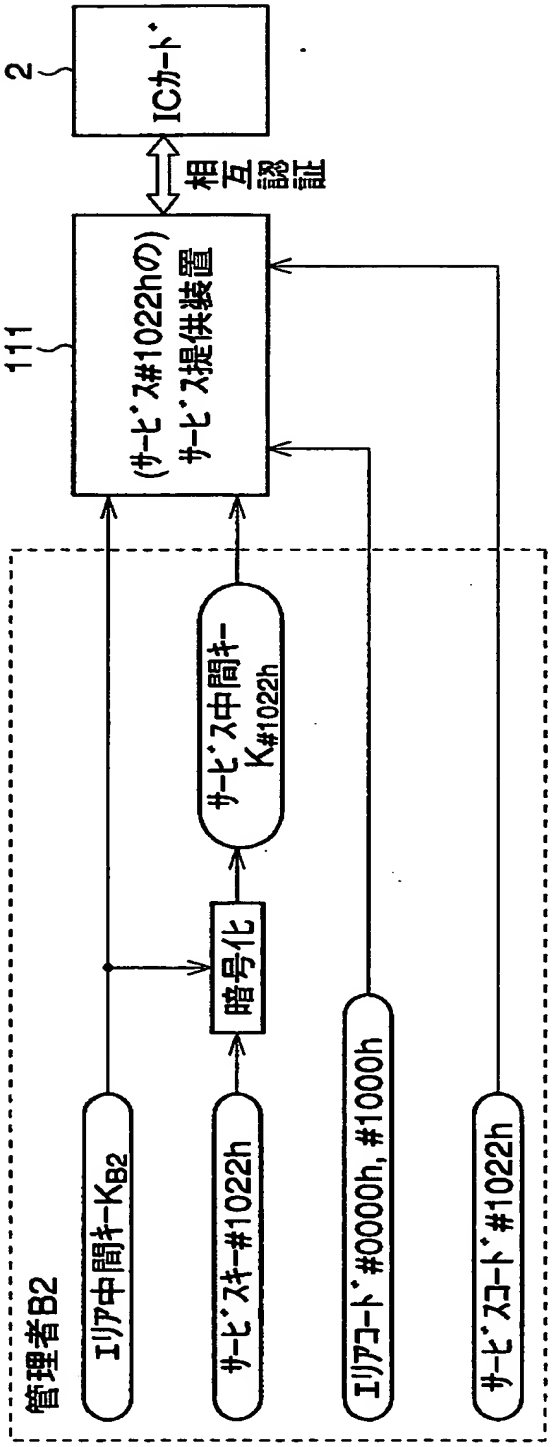
【図12】


ICカード2
サービス提供装置111
乱数
D1
E1
E2
D2
DES (DEC)
DES (ENC)
Kac
Kbc
リーダ／ライタからカードの認証

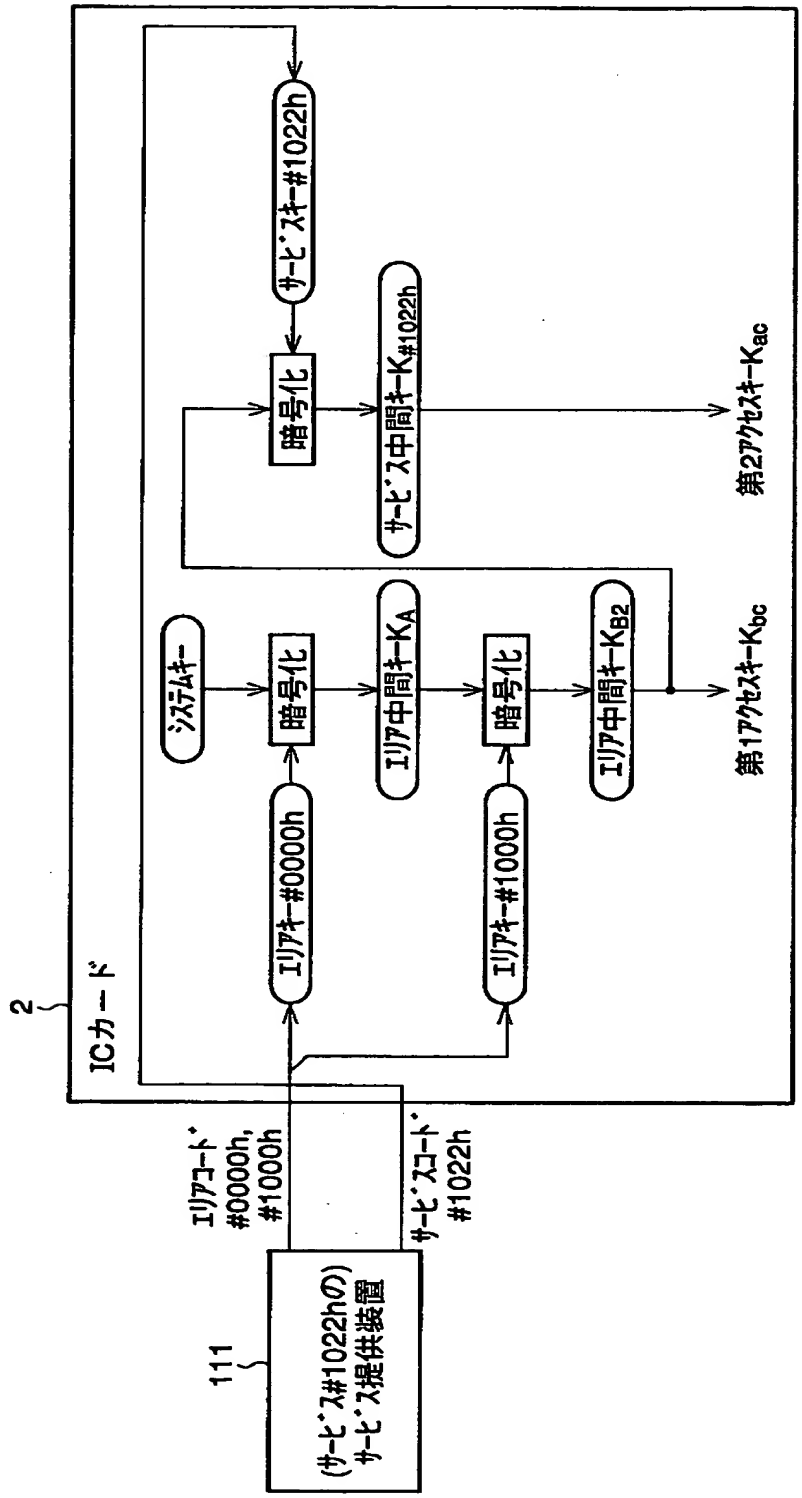
【図13】


ICカード2
乱数
E2
Kbc
Kac
DES (ENC)
DES (DEC)
D1
サービス提供装置111
D2
E1
カードからリーダ／ライタの認証

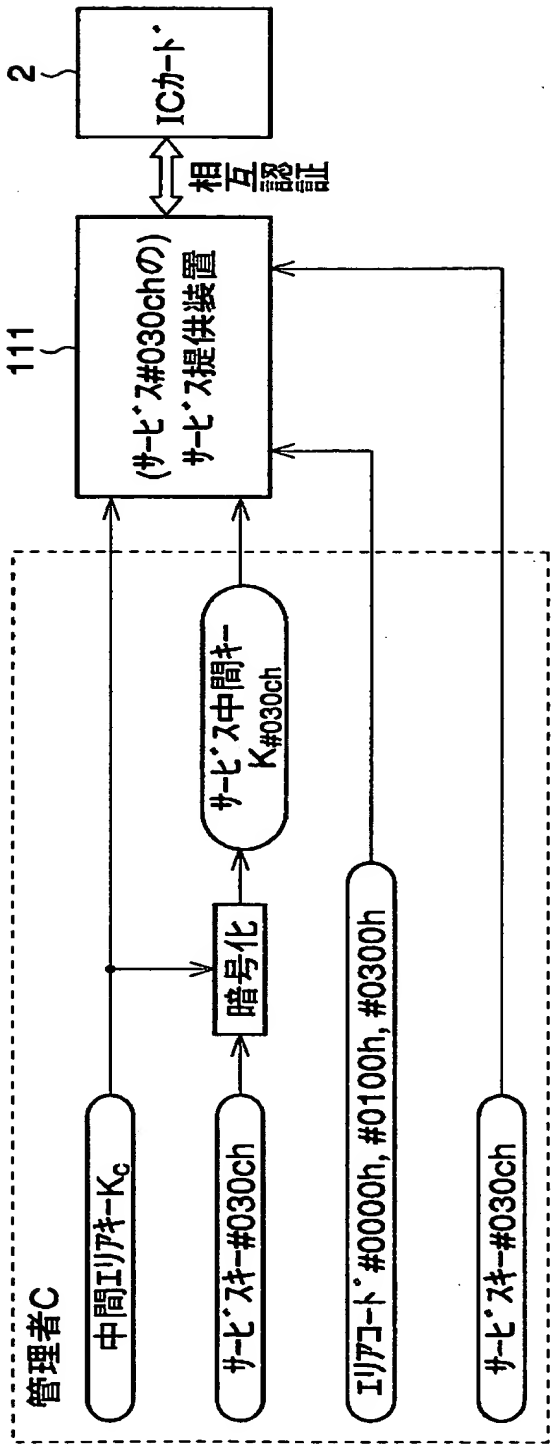
【図14】


2
ICカード
相互認証
111
(サービス#1022hの)
サービス提供装置
管理者B2
Iリア中間キーKB2
サービスキー#1022h
暗号化
サービス中間キー
K#1022h
Iリアコード#0000h, #1000h
サービスコード#1022h

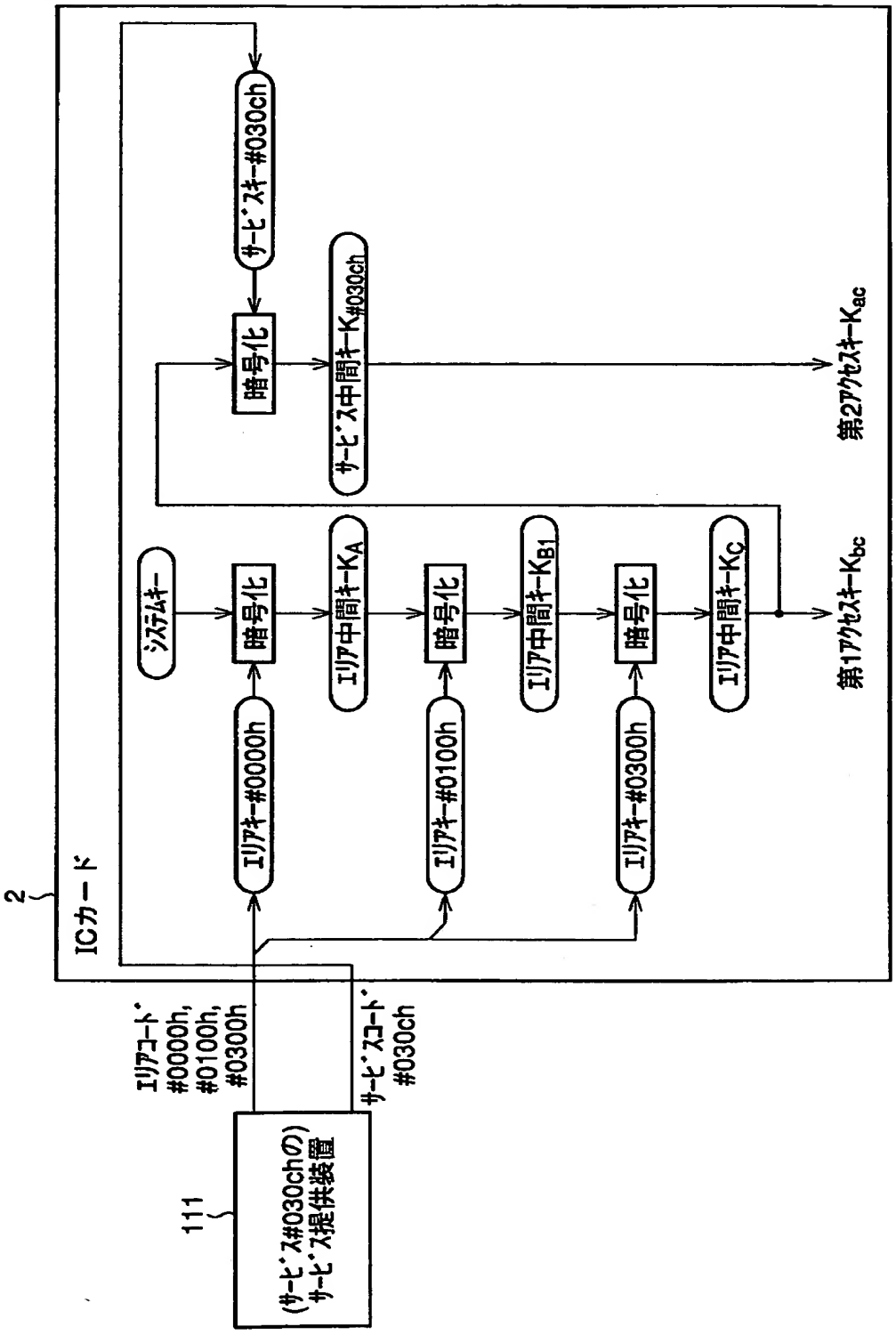
【図15】


2
ICカード
エリアコード
#0000h,
#1000h
サービスコード
#1022h
111
(サービス#1022hの)
サービス提供装置
エリアキー#0000h
エリアキー#1000h
システムキー
暗号化
暗号化
暗号化
エリア中間キーK_A
エリア中間キーK_{B2}
サービス中間キー$K_{\#1022h}$
サービスキー#1022h
第1アクセスキーK_{bc}
第2アクセスキーK_{ac}

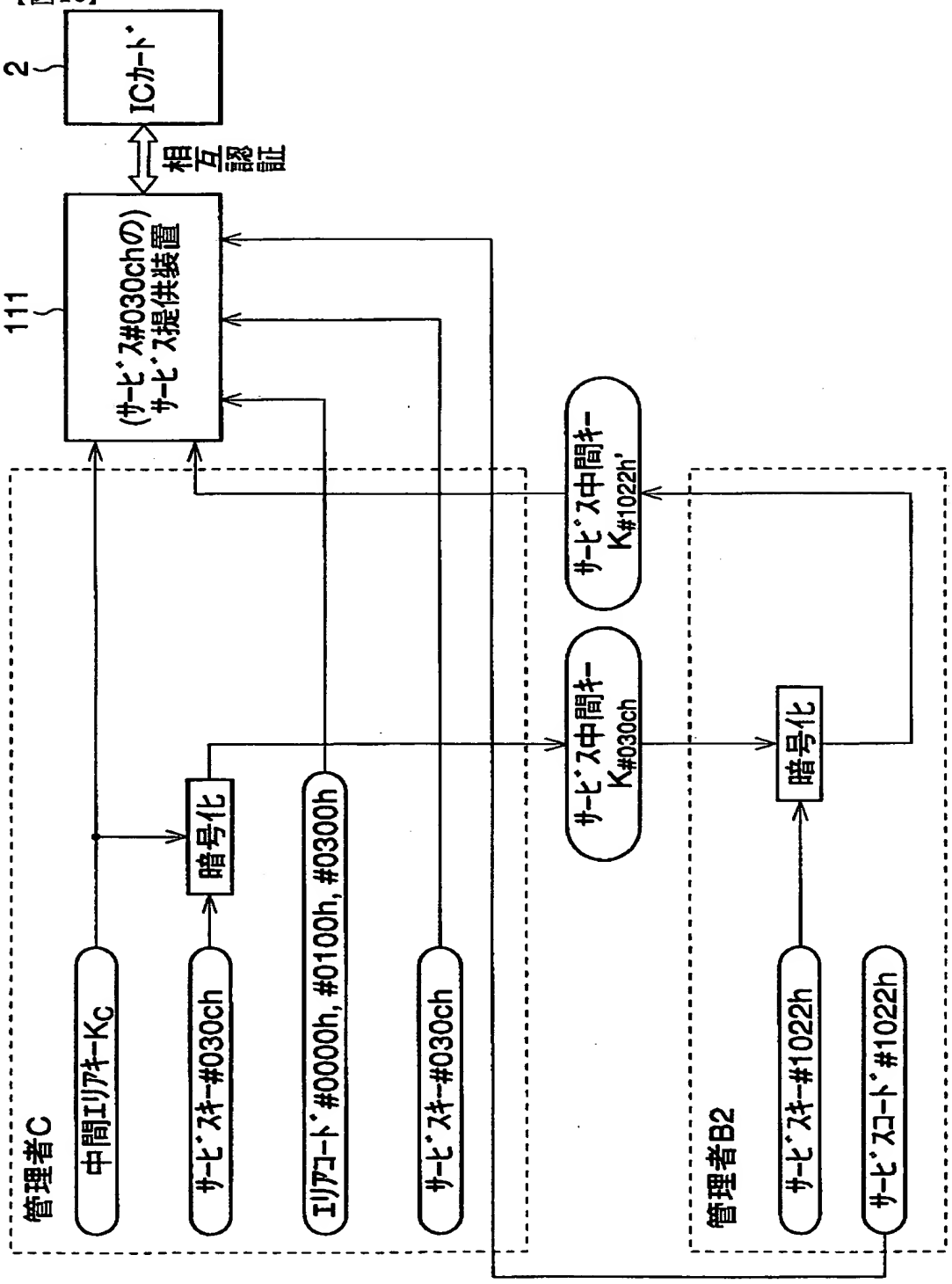
【図16】


2
ICカード
相互認証
111
(サービス#030chの)
サービス提供装置
管理者C
中間IリアキーK_c
サービスキー#030ch
暗号化
サービス中間キー
$K_{\#030ch}$
Iリアコード #0000h, #0100h, #0300h
サービスキー#030ch

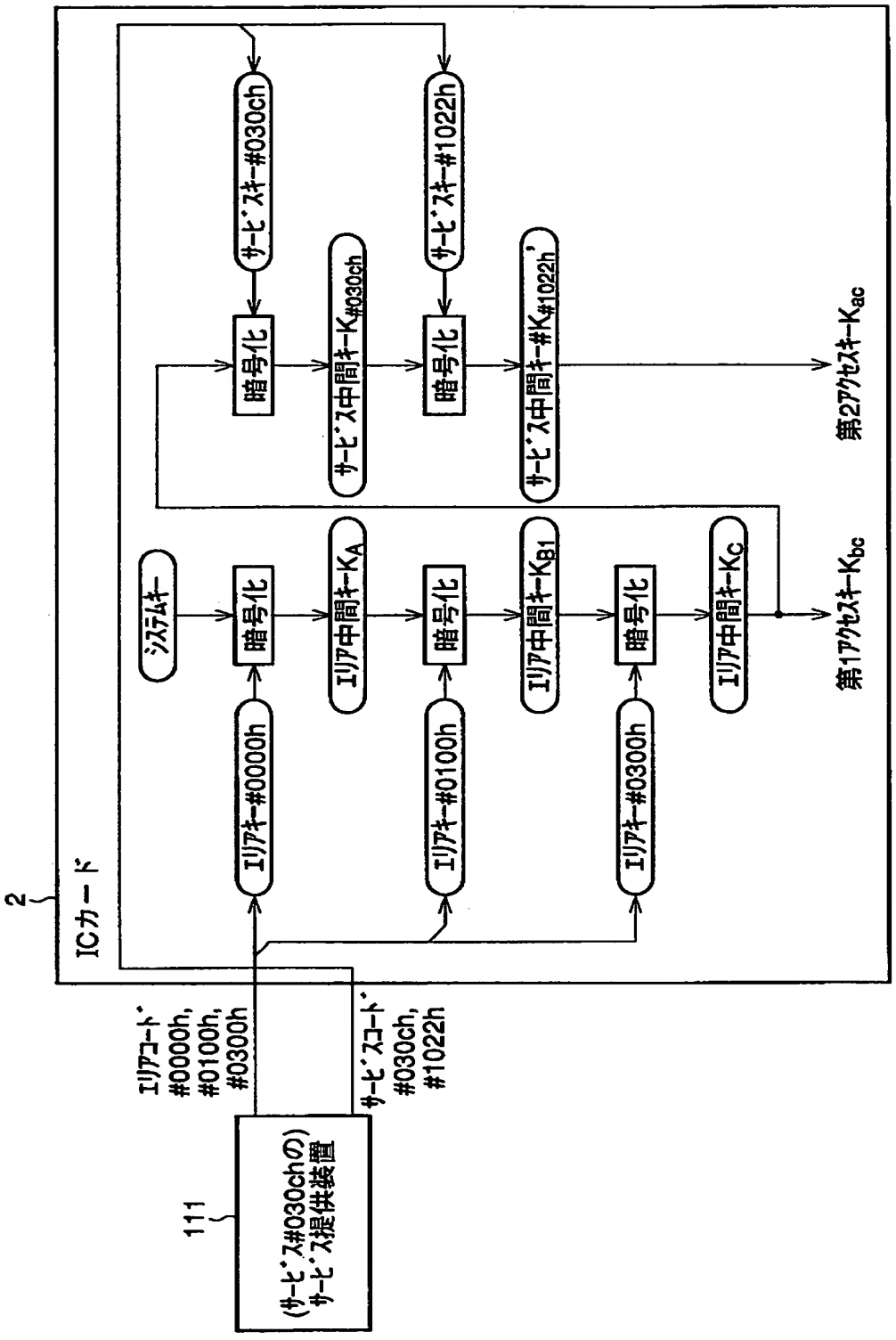
【図17】


2
ICカード
エリアコード
#0000h,
#0100h,
#0300h
サービスコード
#030ch
111
(サービス#030chの)
サービス提供装置
エリアキー#0000h
エリアキー#0100h
エリアキー#0300h
システムキー
暗号化
暗号化
暗号化
暗号化
エリア中間キーK_A
エリア中間キーK_{B1}
エリア中間キーK_C
第1アクセスキーK_{bc}
サービス#030chキー
サービス中間キー$K_{\#030ch}$
第2アクセスキーK_{ac}

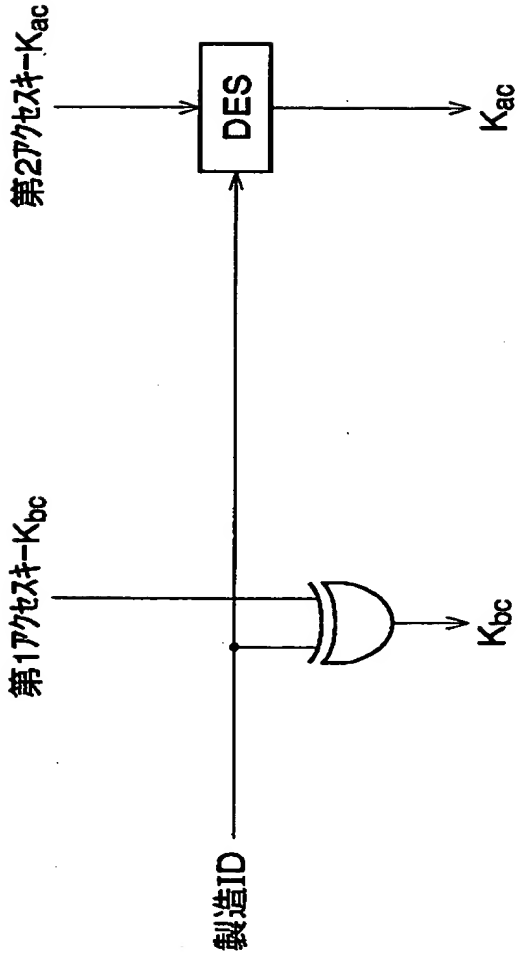
【図18】


2
ICカード
相互認証
111
(サービス#030chの)
サービス提供装置
管理者C
中間Iリアキー Kc
暗号化
サービスキー#030ch
Iリアコード #0000h, #0100h, #0300h
サービスキー#030ch
サービス中間キー
K#030ch
サービス中間キー
K#1022h'
暗号化
管理者B2
サービスキー#1022h
サービスコード #1022h

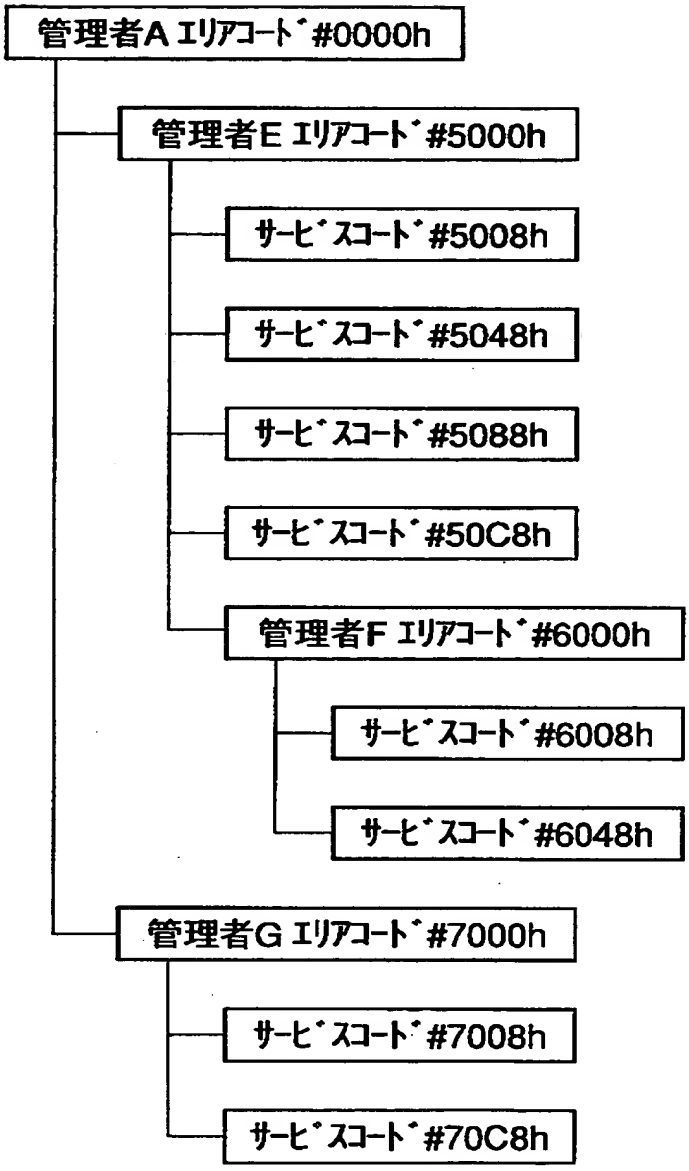
【図19】


2
ICカード
111
(サービス#030chの)
サービス提供装置
エリアコード
#0000h,
#0100h,
#0300h
サービスコード
#030ch,
#1022h
エリアキー#0000h
エリアキー#0100h
エリアキー#0300h
システムキー
暗号化
エリア中間キーK_A
エリア中間キーK_{B1}
エリア中間キーK_C
サービスキー#030ch
サービス中間キー$K_{\#030ch}$
サービスキー#1022h
サービス中間キー$K_{\#1022h}$
第1アクセスキーK_{bc}
第2アクセスキーK_{ac}

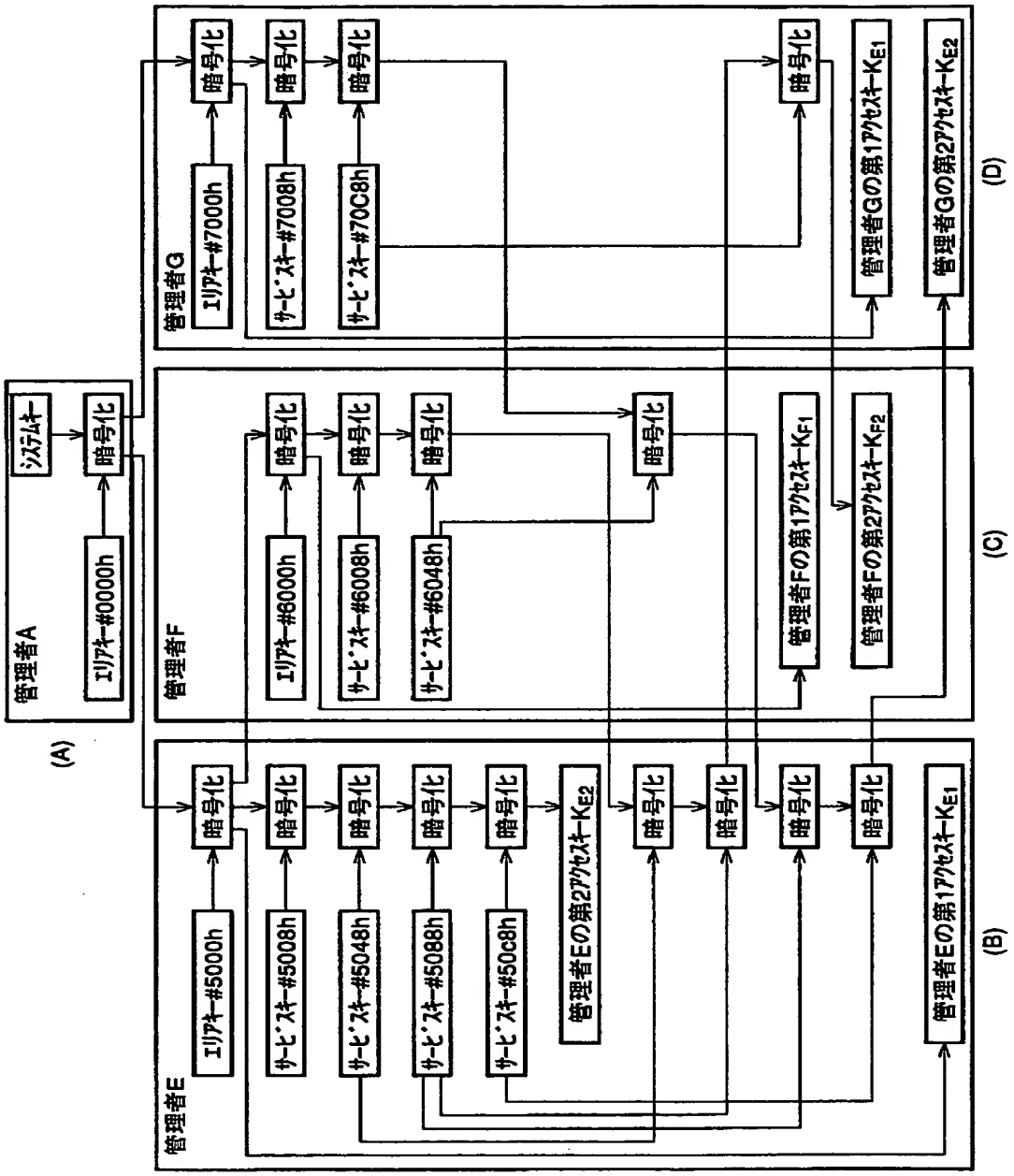
【図20】



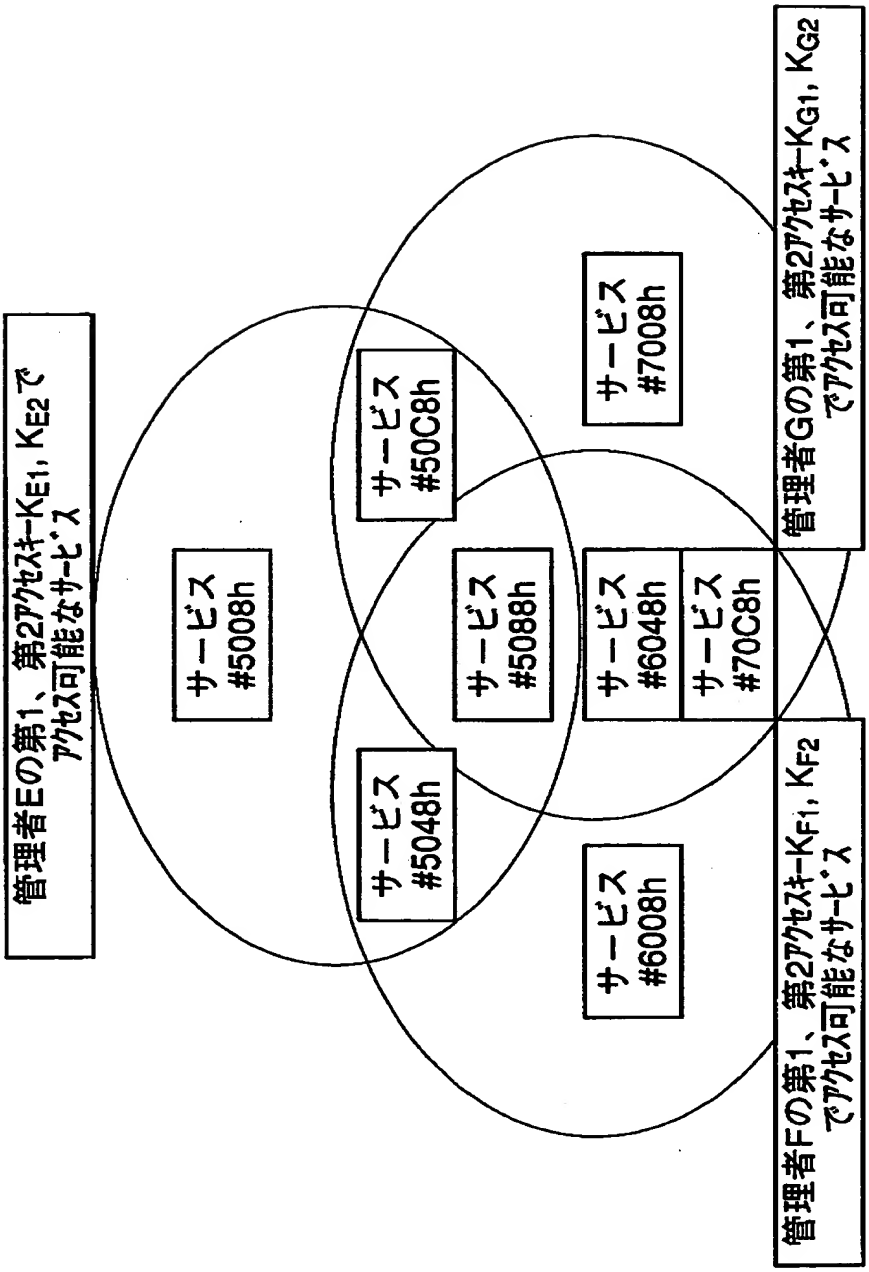
【図21】


管理者A エリアコード #0000h
管理者E エリアコード #5000h
サービスコード #5008h
サービスコード #5048h
サービスコード #5088h
サービスコード #50C8h
管理者F エリアコード #6000h
サービスコード #6008h
サービスコード #6048h
管理者G エリアコード #7000h
サービスコード #7008h
サービスコード #70C8h

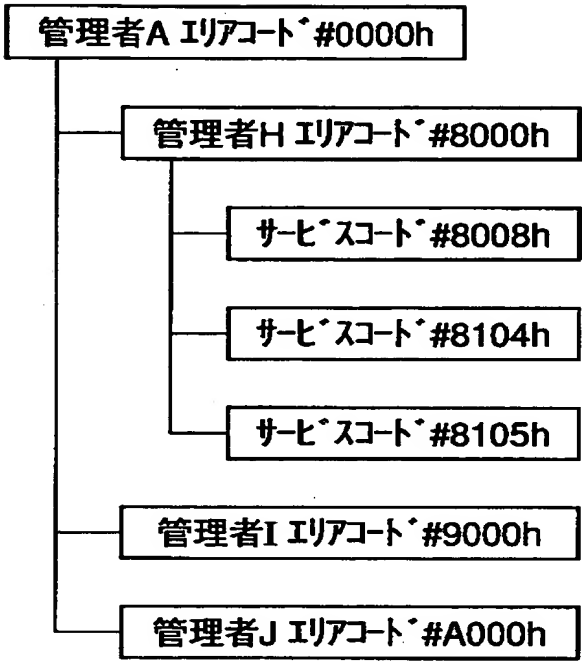
【図22】


管理者A
システムキー
暗号化
エリアキー#00000h
(A)
管理者E
エリアキー#5000h
サービスキー#5008h
サービスキー#5048h
サービスキー#5088h
サービスキー#50c8h
管理者EのKE2
暗号化
管理者EのKE1
(B)
管理者F
エリアキー#6000h
サービスキー#6008h
サービスキー#6048h
管理者FのKF1
管理者FのKF2
(C)
管理者G
エリアキー#7000h
サービスキー#7008h
サービスキー#70C8h
管理者GのKE1
管理者GのKE2
(D)

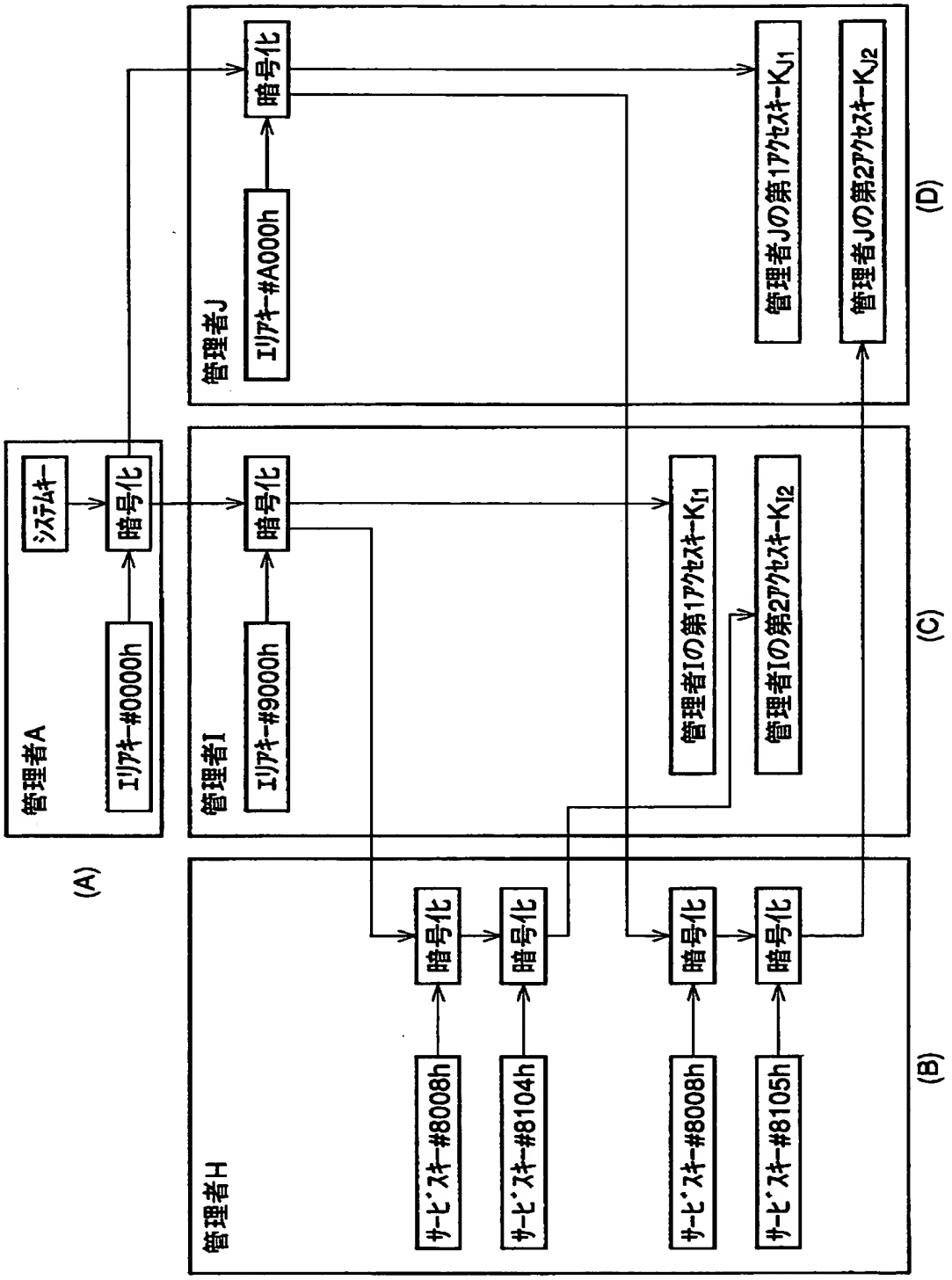
【図23】


管理者Eの第1、第2アクセスキーKE1, KE2でアクセス可能なサービス
サービス #5008h
サービス #50C8h
サービス #5048h
サービス #5088h
サービス #6008h
サービス #7008h
サービス #6048h
サービス #70C8h
管理者Gの第1、第2アクセスキーKG1, KG2でアクセス可能なサービス
管理者Fの第1、第2アクセスキーKF1, KF2でアクセス可能なサービス

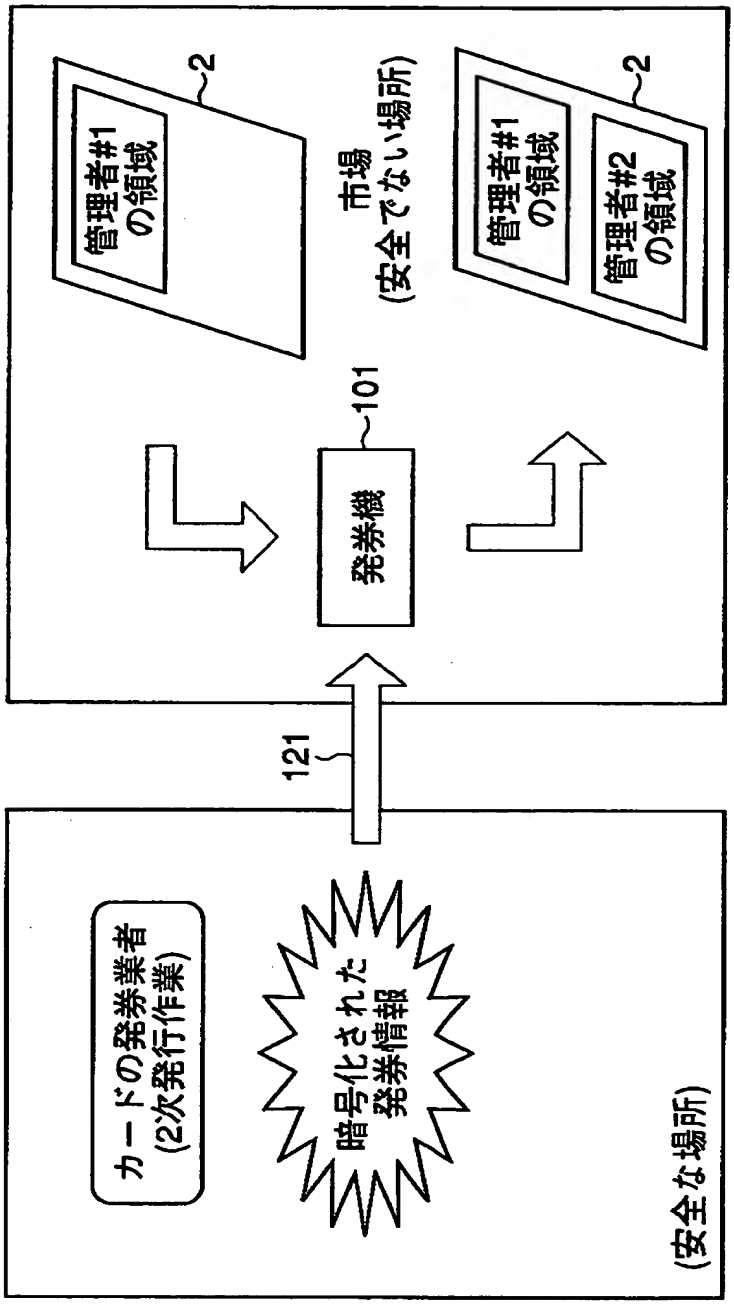
【図24】


管理者A エリアコード #0000h
管理者H エリアコード #8000h
サービスコード #8008h
サービスコード #8104h
サービスコード #8105h
管理者I エリアコード #9000h
管理者J エリアコード #A000h

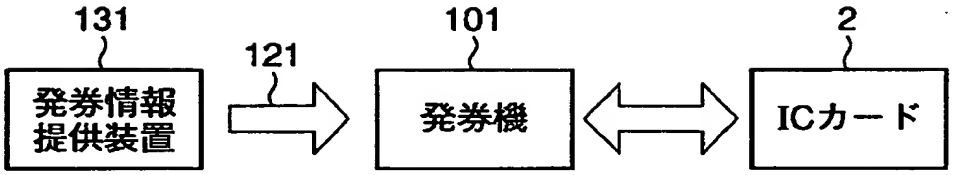
【図25】


管理者A
システムキー
暗号化
Iリアキー#0000h
(A)
管理者I
暗号化
Iリアキー#9000h
管理者Iの第1アクセスキーK11
管理者Iの第2アクセスキーK12
(C)
管理者J
暗号化
Iリアキー#A000h
管理者Jの第1アクセスキーKJ1
管理者Jの第2アクセスキーKJ2
(D)
管理者H
暗号化
暗号化
暗号化
暗号化
サービスキー#8008h
サービスキー#8104h
サービスキー#8008h
サービスキー#8105h
(B)

【図26】

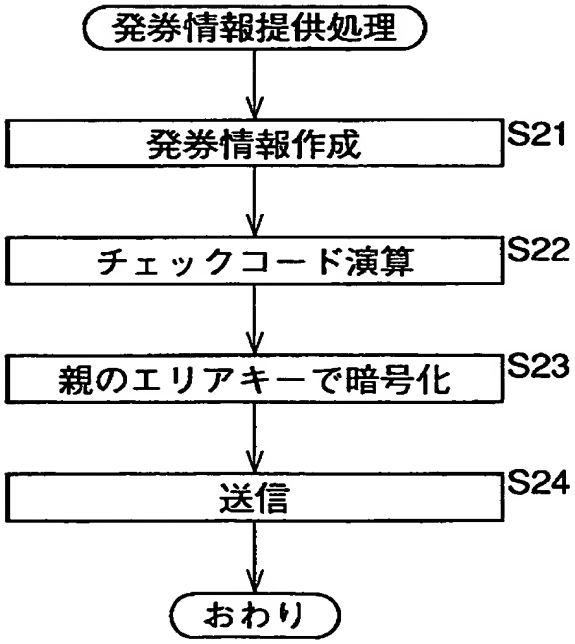

管理者#1
の領域
2
市場
(安全でない場所)
管理者#1
の領域
管理者#2
の領域
2
101
発券機
121
カードの発券業者
(2次発行作業)
暗号化された
発券情報
(安全な場所)

【図27】



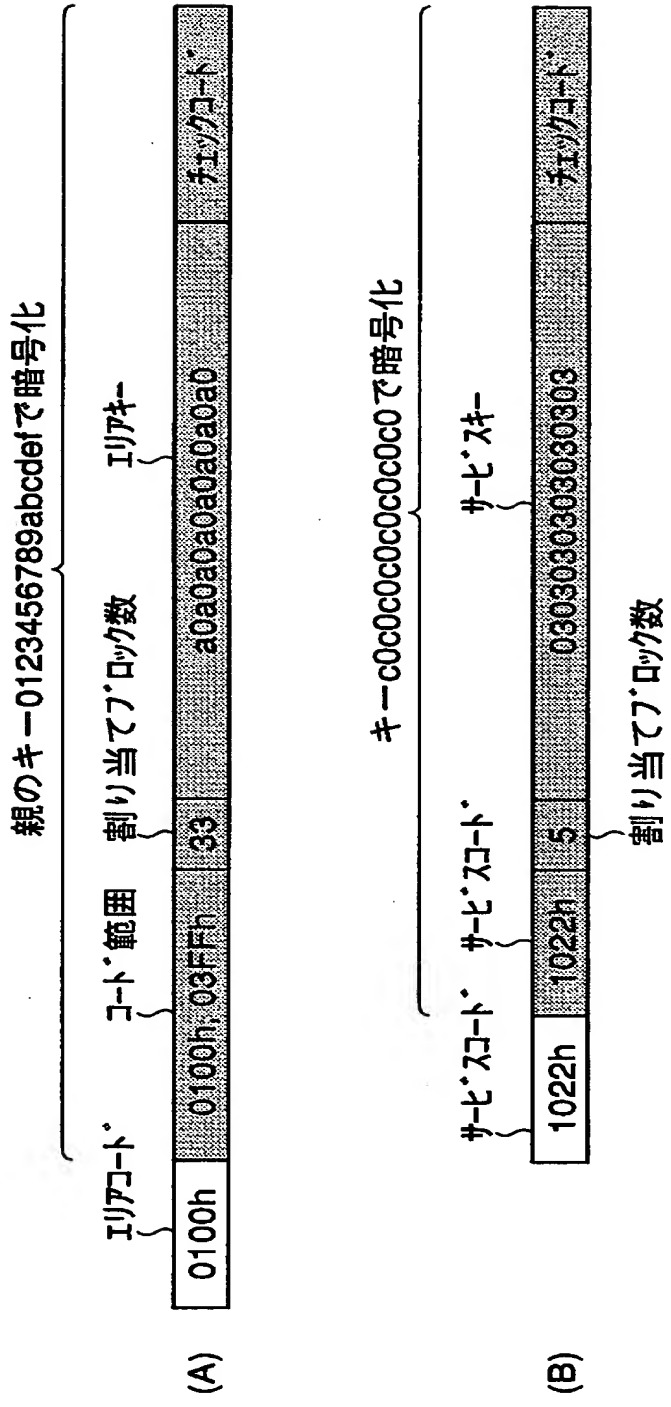
発券処理システム

【図28】

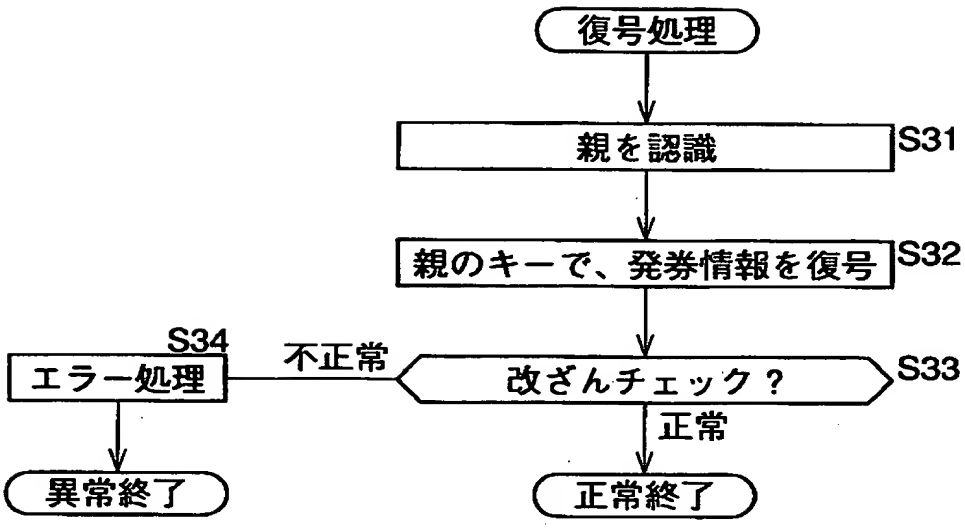


出証特平１１－３０３２４８２

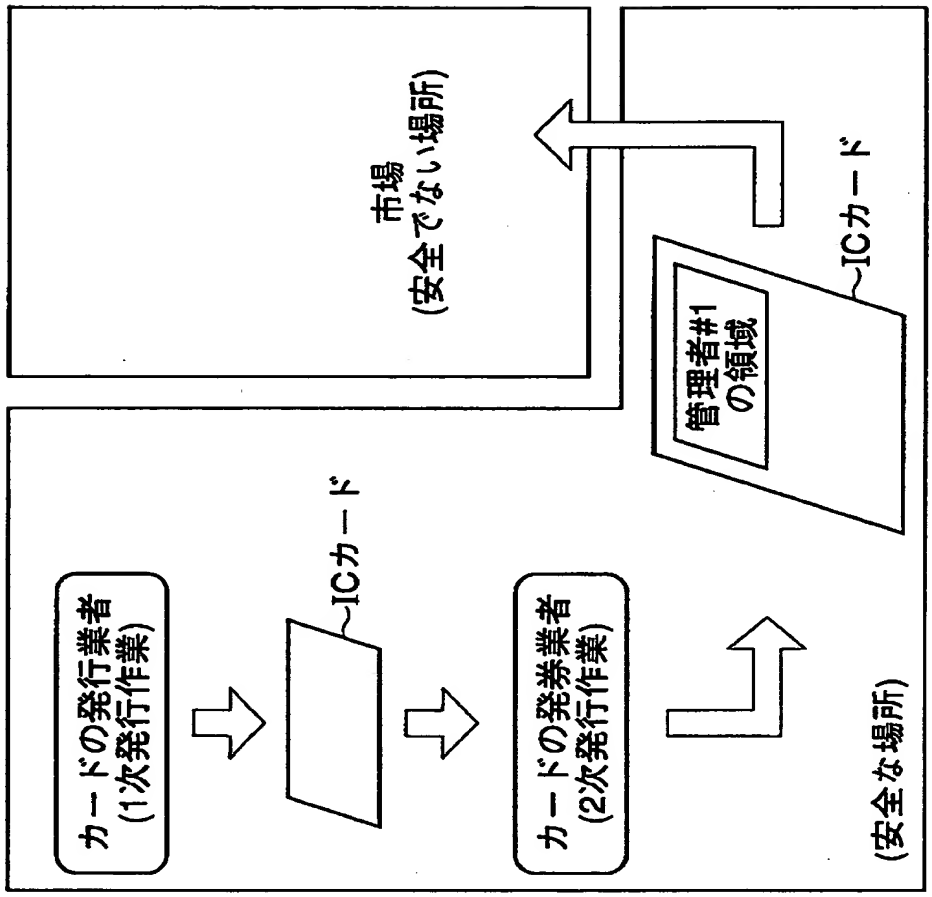
【図29】


親のキー0123456789abcdefで暗号化
エリアコード
コード範囲
割り当てブロック数
エリアキー
0100h
0100h, 03FFh
33
a0a0a0a0a0a0a0a0
チェックコード
(A)
キーc0c0c0c0c0c0c0c0で暗号化
サービスコード
サービスコード
サービスキー
1022h
1022h
5
0303030303030303
チェックコード
割り当てブロック数
(B)

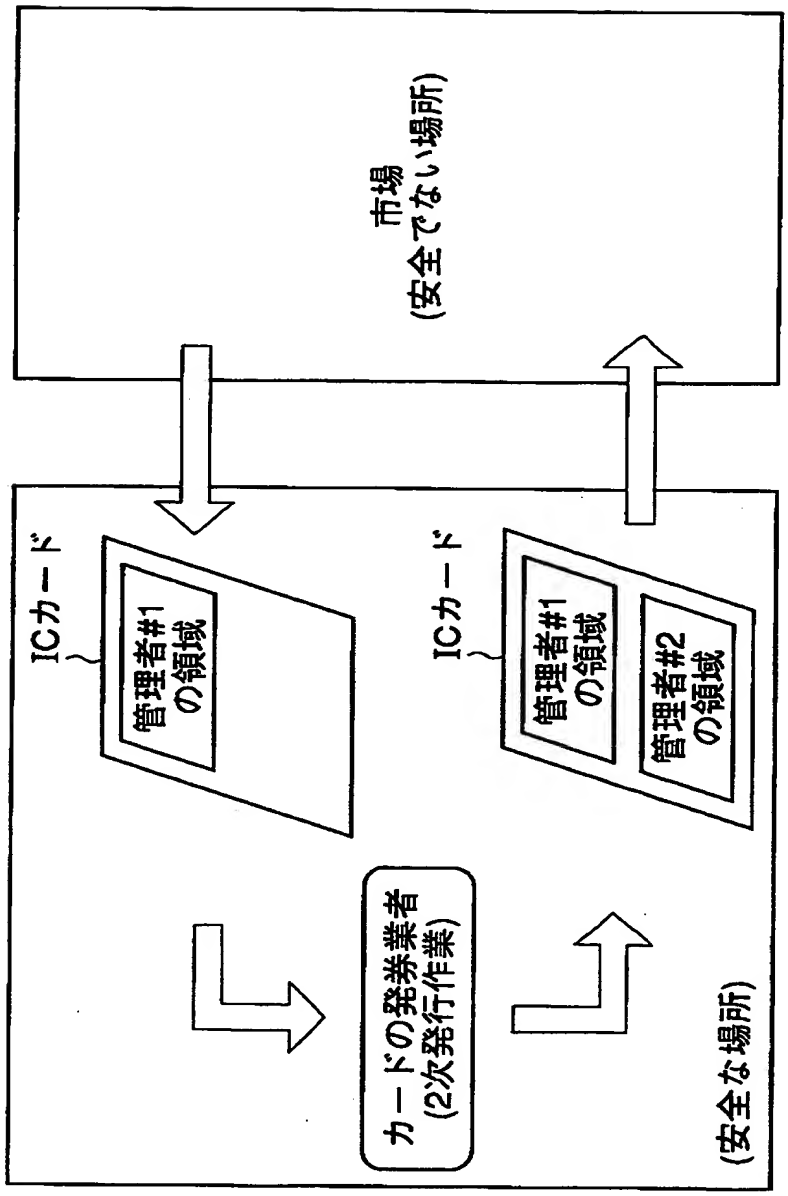
【図30】


復号処理
親を認識
S31
親のキーで、発券情報を復号
S32
S34
エラー処理
不正常
改ざんチェック？
S33
正常
異常終了
正常終了

【図31】


市場
(安全でない場所)
ICカード
管理者#1
の領域
ICカード
カードの発行業者
(1次発行作業)
カードの発券業者
(2次発行作業)
(安全な場所)

【図32】


市場
(安全でない場所)
ICカード
管理者#1
の領域
ICカード
管理者#1
の領域
管理者#2
の領域
カードの発券業者
(2次発行作業)
(安全な場所)

【書類名】　　要約書

【要約】

【課題】　ＩＣカードによるサービスの提供を開始するのに、ＩＣカードに記憶させることが必要な発券情報の改竄や盗聴等を防止する。

【解決手段】　発券情報提供装置１３１では、発券情報が暗号化され、その結果得られる暗号化発券情報が、伝送媒体１２１を介して、発券機１０１に送信される。発券機１０１では、発券情報提供装置１３１からの暗号化発券情報が受信されて登録される。そして、発券機１０１は、ＩＣカード２と通信可能な状態となると、登録されている暗号化発券情報を、ＩＣカード２に送信する。ＩＣカード２では、発券機１０１からの暗号化発券情報が復号され、その結果得られる発券情報が記憶される。

【選択図】　　図２７

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000002185
【住所又は居所】　東京都品川区北品川６丁目７番３５号
【氏名又は名称】　ソニー株式会社
【代理人】　申請人
【識別番号】　100082131
【住所又は居所】　東京都新宿区西新宿７丁目５番８号　ＧＯＷＡ西新宿ビル６Ｆ　稲本国際特許事務所
【氏名又は名称】　稲本　義雄

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社